CRB

CALIFORNIA
STATE LIBRARY
FOUNDED 1850

California Research Bureau
900 N Street, Suite 300
P.O. Box 942837
Sacramento, CA 94237-0001
(916) 653-7843 phone
(916) 654-5829 fax

Public and Private Applications of Video Surveillance and Biometric Technologies

By Marcus Nieto
Kimberly Johnston-Dodds
and
Charlene Wear Simmons, Ph.D.

MARCH 2002

CRB 02-006

CALIFORNIA RESEARCH BUREAU

Public and Private Applications of Video Surveillance and Biometric Technologies

By Marcus Nieto
Kimberly Johnston-Dodds
and
Charlene Wear Simmons, Ph.D.

ISBN 1-58703-153-1

Contents

Executive Summary

At the request of the Senate Committee on Privacy, chaired by Senator Steve Peace, in this report the California Research Bureau (CRB) presents a survey of Close-Circuit Television (CCTV) and biometric security systems used in the United States and in other countries. We find that an increasing number of cities, schools, transit districts and public housing are deploying CCTV surveillance systems to monitor and protect the public. Our first survey, in 1997, found that only 13 city police departments in the country used CCTV video surveillance systems, primarily to monitor pedestrian traffic in downtown and residential districts. Technological advances, declining costs, and heightened security concerns following the September 11, 2001, terrorist attacks have led to rapid diffusion of both CCTV surveillance and biometric technologies. For example, CCTV video surveillance is widely used in public schools to monitor student movement and detect illegal activity, and at street intersections to catch cars running red lights. Private sector applications greatly exceed those in the public sector, including in the workplace, apartment buildings, garages, stores, banks, and restaurants.

Facial recognition systems (biometric technology), when used in conjunction with CCTV video surveillance, offer a partially accurate means to identify potential terrorists and criminals. They operate by comparing scanned faces against law enforcement databases. Perhaps the most well known, and controversial, application of these technologies occurred at the 2001 Superbowl, when law enforcement videotaped fans without their knowledge, and then compared their faces to criminal databases.

While there has been no systematic or focused evaluation of the effectiveness of CCTV surveillance in ensuring public safety, anecdotal information suggests that it does have a chilling effect on crime in targeted areas. However the criminal activities may merely migrate to other locations, leaving the total crime rate the same.

The application of these technologies raises important legal issues. These include potential chilling effects on First Amendment freedoms of speech, petition and assembly, and questions about the limits of Fourth Amendment protections against unreasonable searches and seizures. The report also analyzes pertinent sections of the newly enacted federal *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (the PATRIOT Act). These sections of the PATRIOT Act are central to the debate surrounding global use of emerging surveillance technologies, law enforcement, national security interests and the privacy rights of citizens. The speed at which CCTV and biometrics technologies are evolving, and their rapid diffusion, challenge the ability of both judicial and legislative decision-makers to enact and enforce policies that protect the public's security and right to privacy.

Overview of CCTV Video Surveillance and Biometrics

TECHNOLOGICAL INNOVATIONS AND EXPANDING USE

In 1997, the California Research Bureau (CRB) examined the potential of Closed Circuit Television (CCTV) technology to improve public safety through remote surveillance.[1] Businesses such as banks were early adopters of CCTV for crime detection and prevention purposes. Our review found that an increasing number of cities, schools and residential districts were deploying CCTV systems. Shortly thereafter, many schools installed CCTV systems in response to violent outbreaks such as at Columbine High School. Now new CCTV technological features, and an urgent need for enhanced public security following the September 11, 2001, terrorist attacks, are leading to a rapidly expanding use of CCTV and a related technology, biometrics.

There appears to be considerable public support for this expansion. A *Business Week* survey conducted a week after the September 11 terrorist attack found that 63 percent of the adults surveyed were in favor of expanded camera surveillance on streets and in public places, and 86 percent were in favor of using facial recognition technology to scan for suspected terrorists at various locations and public events.[2] CCTV surveillance increases the "eyes" of law enforcement: "You don't need 4,000 FBI agents on the streets when you've got 4,000 video cameras on the streets that can recognize people," according to Howard Levinson, a security expert and consultant."[3]

Most public and business-related CCTV video surveillance systems are *actively* monitored by security personnel in a centralized setting, *remotely* monitored, monitored over the Internet through video streaming, or *passively* taped for future viewing if needed (such as in the event of a bank robbery). Relatively new features in CCTV surveillance technology that considerably enhance its power and scope include night vision cameras, computer-assisted operations, and motion detectors that allow an operator to instruct a system to go on "red alert" when anything moves in view of the cameras.

CCTV camera in downtown Sacramento, California

Video equipment technologies can be activated by motion detectors and/or recording images, even at night. Infrared high sensitivity equipment and surveillance systems operate outside of the visible light spectrum. Examples include Forward Looking Infra-red Radar (FLIR), that is able to detect activity behind walls, and infrared (IR) thermal imaging cameras that are able to detect activities in darkness. Local law enforcement and Immigration and Naturalization Service (INS) police use motion-activated IR thermal imaging surveillance cameras along the U.S.- Mexican border. According to INS officials, IR cameras detect the invisible infrared energy that all people and objects emit, and can "see" better than the naked eye at night and in bad weather. Since the energy being sensed is heat and not light, thermal images can be used in both daytime and nighttime operations. The INS uses the cameras primarily at night to detect suspects crossing the border.[4] Another use of IR thermal imaging cameras is to assist night search and rescue missions by both civil and military personnel.

New models of CCTV cameras are equipped with bulletproof casing and automated self defense mechanisms to protect camera lenses. Picture clarity is equal to digital compact disk quality-- many cameras are able to read a cigarette package label at a hundred meters. Cameras are also becoming smaller, making it easier to conceal the equipment. A CCTV camera can be hidden almost anywhere in the workplace and even worn on clothing. These little devices are capable of zooming in on the smallest of details, and they can pan and tilt. Equipment costs have decreased to the point where a business might recoup its investment by cutting losses due to stealing, or by discouraging unproductive worker down time. Also, the threat of industrial espionage has prompted many companies to resort to video surveillance to protect proprietary technologies.

CCTV technology converges with sophisticated software, capable of recognizing facial features automatically, analyzing crowd behavior, and scanning the area between skin surface and clothes. The advent of new biometric software technologies, especially computerized facial recognition used in conjunction with CCTV surveillance systems, can facilitate law enforcement's ability to identify suspected terrorists or criminals. Law enforcement conducts this process by comparing pictures and known facial features against national and international databases.

CCTV Surveillance and Biometrics

Biometrics is a term that applies to the many ways in which human beings can be identified by unique aspects of the body. Fingerprints are the most commonly known biometric identifier. Other biometric identifiers include hand prints, vein dimensions, iris (eye) designs, the pattern of blood vessels in the retina, body odors, characteristic and unique movements, individual voices, and of course, DNA. Countries around the world are implementing biometric surveillance schemes. Spain has begun a national fingerprint system to track recipients of unemployment benefits and healthcare entitlements. Russia is developing a national fingerprint system for its banks to prevent fraud. Jamaicans scan their thumbs into a database before qualifying to vote at elections. France and Great Britain are testing equipment that encodes individual fingerprint information onto credit cards.[5] In a recent talk on border security in San Diego, Doris Meissner, former head of the U.S. Immigration and Naturalization Service, said that, "We are increasingly going to

be asking for biometrics from those of us in the law abiding public, in order to facilitate our being able to carry on our normal lives…"[6]

The technical definition of a biometric is "any *measurable, robust, distinctive, physical characteristic* or *personal trait* of an individual that can be used *to identify, or verify* the claimed identity of that individual."[7] Every biometric system contains three components:

- Enrollment – the process of collecting biometric samples
- Templates – the data that represents the enrollee's biometric located in a database
- Matching – the process of comparing a submitted sample against one (verifying) or many (identifying) templates in the database[8]

Facial Recognition Identification versus Verification

Biometric identification or verification systems are distinct from each other. Facial recognition identification systems are being combined with CCTV surveillance to identify suspected criminals and terrorists in airports and at border crossings. Combined biometric verification systems and CCTV are used to control access to computers, secured areas and to verify passport information or citizenship status.

When facial recognition technology is used to *identify* an individual, the system attempts to answer the question "*Who is John Doe*?" by reading the information or sample provided and comparing it to many templates in the database. It then reports or estimates who the person is from its database. When the technology is asked to *verify* someone, the system is asked "*Is this John Doe*?" (after the individual claims to be John Doe). It then compares the biometric information presented to the template in the database identified as John Doe and either accepts or rejects the claim.

Templates in a facial recognition database typically are composed of complex programmed knowledge rules, statistical decision rules, neural networks and algorithms.[9] This means that the database is built using certain assumptions that introduce the potential for errors. In other words, facial recognition database templates do not contain exact likenesses of individuals but rather complex statistical and mathematical estimates of digitized images.

Evaluating Performance of Facial Recognition Technologies

Since identification and verification systems are different, so too are the performance measures and protocols used to evaluate the efficacy of each type of system. For *identification* systems, the principal measure "equals the percentage of queries in which the correct answer can be found in the *top few matches*."[10] In other words, the higher the percentage of a correct match contained within the top *matches*, the better the system. Thus, if used to attempt to capture terrorists or criminals in public places, the data input would be an image captured on CCTV, and the output from the database would be a list of top matches. The sheriff or airport security guard then would make a subjective decision to further search or detain the individual.

Two error statistics, false-reject rate and false-alarm rate, are used to measure the ability of a verification system. "A false reject occurs when a system rejects a valid identity (i.e., the real Michelle Kwan is denied access to the Olympic skating rink); a false alarm occurs when a system incorrectly accepts an identity."[11]

In general, experts and researchers report that face recognition algorithms are sensitive to changes in illumination, such as shifting sunlight during the day, and changes in facial positions.[12] A systems' performance will drop significantly if the algorithms are not corrected to address lighting variations and moving faces.

Application of Surveillance Technologies and Concerns of Misuse

The recent use of facial recognition technology at the 2001 Super Bowl is a good example that encapsulates these emerging technologies, their use in law enforcement surveillance, and the debate over potential misuse. In January 2001, the faces of over 100,000 fans entering the stadium to watch the Super Bowl in Tampa, Florida, were recorded by local law enforcement on video cameras. The facial images were then digitized by sophisticated software,* and checked electronically against a criminal computer database. Fans were not aware that this had occurred until after it was reported in the national news.[13] Law enforcement officials maintained that they were using the latest available security tool, and that it was no more intrusive than a video camera in a convenience store.[14] Soon after the 2001 Superbowl, CCTV surveillance, combined with biometric technology, was adopted for use on the streets of the cities of Tampa Bay and Virginia Beach (see page 12 for discussion).

Americans are of two minds about the rapid evolution of CCTV and biometric security and surveillance systems. Polls suggest that they are willing to give up some privacy if that is the price for better security.[15] Conversely, there is a widespread belief that information obtained from video surveillance and biometric devices could be abused by government agencies, employers or businesses. For example, if facial recognition software and CCTV cameras are used together, and linked to public databases such as pictures on file in a state motor vehicles department, then individual faces could be identified, tracked, recorded, and stored into other databases by the government, or perhaps sold to private industry.[16] Lack of surveillance disclosure, such as at the Super Bowl, is another concern.

The narrow accuracy range of the technology also raises concerns about false identification. A recent study by the National Institute of Standards and Technology found that when digitized posed photos of the same person taken 18 months apart were compared, they triggered a false rejection by computers 43 percent of the time.[17] With such a large potential error rate, law enforcement relying solely on these technologies to identify individuals might often stop and question an innocent person instead of a possible criminal suspect.

* The software was developed by scientists at the Massachusetts Institute of Technology in the early 1990s using federal funds provided by the Department of Defense. See "Winter Olympics Group is Considering Super Bowl's Controversial Surveillance," *Wall Street Journal*, February 5, 2001, B13.

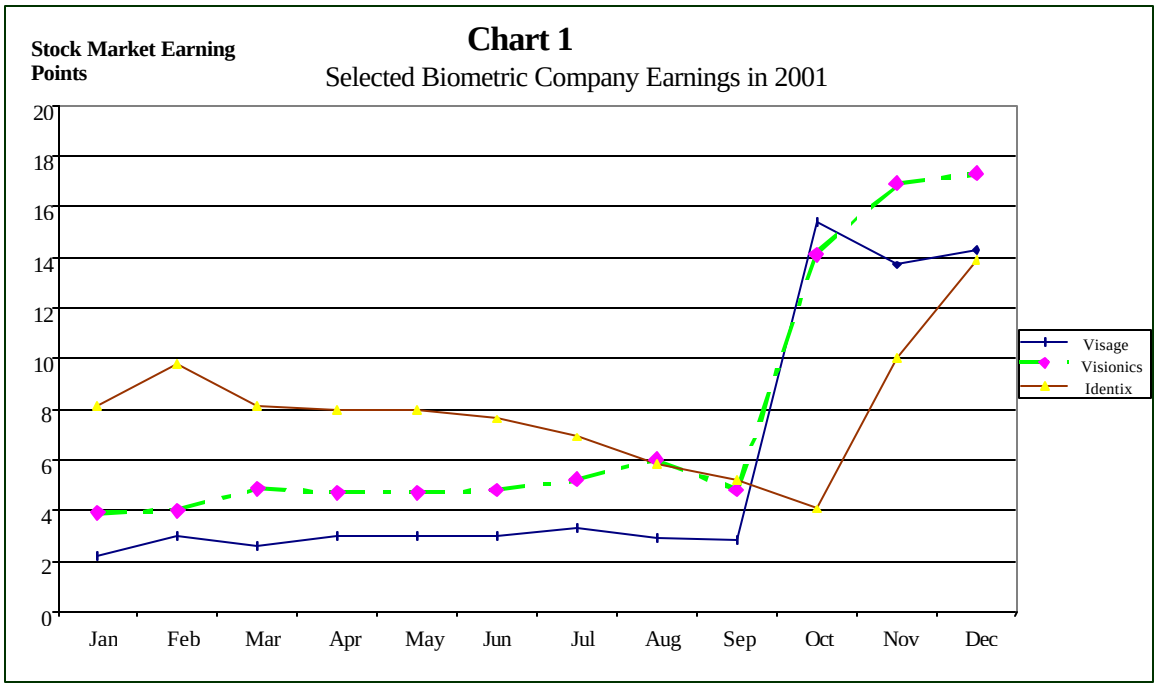
Security systems that combine video and facial recognition technologies have been used in the casino industry in Atlantic City and Las Vegas for several years. One industry firm estimates that over 100 casinos nationwide have facial biometric systems in place.[18] When used in conjunction with casino CCTV cameras and computer databases containing "cheater" information, facial biometrics may identify a known cheater in seconds. According to one casino official, "We have about 10,000 photographs of cheaters, people who have been arrested, evicted or ejected from this or other casinos. We put no people in here [the database] who are honest customers or good players. This is specifically for people who could harm us."[19] However one gaming company's marketing brochure touts its "patron management" capabilities that appear to track more than "cheaters." The brochure states that, "player workbooks are loaded with easy-access data that provide the information needed to make the right decision for each player. Colorful icons cue floor personnel on important events such as a birthday, bad address, abandoned card, to name a few." The brochure also advertises the ability of its patron management database to seamlessly integrate with "property management systems, points of sale systems, and third party gaming rating systems."[20]

Biometric systems are being tested at Boston's Logan International Airport and Providence's T. F. Green Airport. In California, the Fresno International Airport and Oakland International Airport are using CCTV surveillance combined with facial recognition technologies.[21] Other uses of facial recognition technology include:

- *Law Enforcement:* Minimizing victim trauma by narrowing mug shot searches, verifying identity for court records, and comparing school surveillance camera images, for example, to known child molesters
- *Security/Counterterrorism*: Controlling access to restricted areas, comparing surveillance images to known terrorists
- *Immigration:* Enabling rapid progression through Customs
- *Correctional Institutions*: Tracking inmates and restricting employee access
- *Schools and Day Care*: Verifying the identity of individuals picking up children
- *Missing Children, Runaways*: Searching surveillance images over the Internet for missing children and runaways
- *Residential Security*: Alerting homeowners of approaching people, restricting access to gated communities
- *Internet E-commerce*: Verifying consumer identity for Internet purchases
- *Healthcare, Benefit payments, Voter verification, Banking*: Minimizing fraud by verifying identity

The demand for facial recognition technology has grown dramatically since September 11, 2001. Robert McCashin, chief executive of Identix (a biometrics company), maintains that, "we've always said that some event would have to happen to propel the technology to the forefront." The terrorist attack opened the "floodgates" for companies to market these technologies.[22] Currently, there are about 200 companies in the U.S. involved in producing biometric security and identification technologies. Since the September 11th attacks, stock prices in the biometric industry generally have increased from an average price of about $4.00 a share to $12.00 a share (See Chart 1). Gross sales

from the security-oriented core of the biometric industry are expected to grow from $400 million in 2000 to $1.9 billion in 2005.[23]



Source: *New York Times*, Stock Market Report, December 17, 2001

However the limitations of facial recognition technologies may restrict their use. There are examples in which law enforcement officials have investigated their capabilities and decided against using them. Most recently, news sources reported that law enforcement in charge of security at the 2002 Olympics in Salt Lake City decided against using the technology in all the venues, including the Olympic hockey arena. The agencies in charge of security complained that it worked too slowly and was not reliable.[24]

INTERNATIONAL APPLICATIONS OF CCTV SURVEILLANCE

In response to crime and potential terrorism, and as a deterrent, many countries employ public video surveillance to monitor population movements. The United Kingdom (UK) has perhaps the most widespread use of CCTV video surveillance. A 1995 research survey found that the UK public generally accepted CCTV public surveillance because of experiences with previous terrorist acts and concerns about random acts of violence.[25] Government officials contend that most people in the UK still support extensive video surveillance in their society because they believe it reduces crime and traffic accidents.[26]

Surveillance cameras are a fact of contemporary life in the United Kingdom. According to one London newspaper, during the course of a 24-hour period, if a person shops, rides a train, buys gasoline, visits a post office, bank, or building, attends a soccer game, or just strolls down the street, then probably several video tapes will record their image.[27] By one estimate, the average Briton is now photographed by 300 separate cameras in a single

day.[28] An American news reporter commented on a recent television program that, "the British are so crazy about their cameras, they're even installing them on London's famous double-decker buses. There will be one on the upper deck and two on the lower levels to keep a watchful eye on bus riders."[29]

Public video surveillance began modestly in 1986, with three CCTV video surveillance cameras installed within a single square mile industrial estate outside the English town of King's Lynn. The area had experienced a number of crimes in previous years, mostly vandalism. In the two years following the installation of the cameras, authorities reported that no crimes were committed.[30] This success in reducing petty crime caught people's attention. By the end of 1994, over 300 jurisdictions in the country were using some form of public video surveillance.[31]

Now, between £225 million to £450 million a year are spent on CCTV cameras installed in shopping areas, housing estates, car parks, and public facilities in many towns and cities. According to one estimate, cameras are so prolific and attached to many different surveillance systems that the actual number might be closer to 1.5 million surveillance cameras in over 400 communities.[32]

In contrast to the rapid diffusion of CCTV surveillance in the UK over the last decade, independent research evaluating its impact and effectiveness is just starting to emerge. Criminology experts and social scientists point out that simply comparing crime statistics (before and after deployment of the cameras) does not measure the complexities. In particular, crime may be merely displaced or diffused from one location to another.[33] More fundamentally, experts and researchers contend that, "CCTV is about far more than just crime prevention; it is about the power to watch and potentially intervene in a variety of situations, whether they be criminal or not…the question of who and what is watched and what warrants intervention have largely been ignored by existing research."[34] Researchers have raised three questions that they have begun to focus on answering:

- Is monitoring certain street populations random or are some social groups more likely to be watched than others?
- To what extent does CCTV operate as an "exclusionary mechanism," targeting the undesirable as well as the criminal, with the goal to remove both from urban areas?
- Does CCTV lead to a form of "social control" by recording more examples of "officially deviant behavior" that is not illegal, and/or responding to larger numbers of petty crime?[35]

Researchers also question the methodology used by law enforcement, industry and newspapers to affirm that there is overwhelming public support of CCTV surveillance: "the vast number of evaluation schemes that have been carried out to date have been undertaken by those with an interest in promoting the cameras and have been technically inadequate."[36]

The social complexities of crime make conducting unbiased, comprehensive evaluations difficult. Nick Tilley, a Sociology Professor at Nottingham Trent University, has conducted research on CCTV for the Home Office Police Research Group in London. Professor Tilley points out that different measuring methodologies produce different results depending on the data used and the questions asked, as the following examples suggest.[37]

- Natural fluctuations in local crime rates make understanding actual effects or changes difficult.

- Floor effects (starting with a very low crime rate area as a study site) make it difficult to measure how much CCTV further reduces crime.

- Other non-crime related changes in the area monitored by CCTV may impact a study's findings.

- Law enforcement, with a vested interest in using CCTV, operates the equipment and reports and records the data, so independent changes in patterns of crime reporting and recording may be difficult to detect.

- CCTV often is part of a system of crime prevention measures, making it difficult to independently isolate and measure only the effect of CCTV.[38]

While Britain currently is the international leader in implementing CCTV, Singapore, Canada, the U.S., Australia, and other European countries have also installed thousands of cameras in public urban settings. However, the public, some government officials, and various organizations in several countries are increasingly concerned about protecting individual privacy. For example, in Canada, the Privacy Commissioner, serving as a public ombudsman, recently issued a finding that criticized the extensive use of CCTV by the city of Kelowna. He found that the city had violated Canada's *Privacy Act,* stating,

> If we cannot walk or drive down the street without being systematically monitored by the cameras of the state, our lives and our society will be irretrievably altered. The psychological impact of having to live in a sense of constantly being observed must surely be enormous, indeed incalculable. We will have to adapt, and adapt we undoubtedly will. But something profoundly precious-our right to feel anonymous and private as we go about our day-to-day lives will have been lost forever.[39]

Since the United Kingdom has a longer, and more widespread, experience with CCTV surveillance cameras, there is a broad debate on their use. One concern is that there are no controls in British law that regulate the purchasing and showing of footage obtained from public CCTV surveillance. Therefore, individuals have no recourse against local government agencies that provide revealing tapes to producers.[40] Since the UK has more CCTV coverage per capita than any other country in the world, it is relatively easy to find footage containing individuals engaged in private activities in parking garages, housing

developments, department stores and offices. Surveillance cameras capture couples intertwined in office stockrooms, elevators and cars; women undressing in department store changing rooms; and husbands and wives in domestic squabbles.
Voyeuristic use of CCTV footage is a major concern. Such footage has been used or sold commercially in video stores all over the UK, according to members of British Parliament's Media Committee. One such video, entitled "Really Caught in the Act," included sex acts and other intimate contacts, recording both benign and illegal activities. The tape prompted outrage in Parliament and protests from civil liberties groups. A spokesperson for a civil liberties group stated that "there are no controls at all. We think it's quite appalling that members of the public can be caught like this."[41] Selective or targeted camera surveillance is another concern, particularly among black men, who are concerned about racial profiling.[42]

CCTV Video Surveillance by U.S. Law Enforcement, Cities, Transit Districts, Public Housing Authorities and School Districts

In 1997, a CRB study located 13 U.S. cities with CCTV street surveillance programs.[43] Recently we undertook to update this information by contacting those cities and other cities mentioned in the press or by knowledgeable observers. We found that the number of cities using CCTV street surveillance systems is increasing, as described in Table 1, but the exact number is unknown. While there is no official record of such programs, according to a survey conducted by the International Association of Chiefs of Police, over 200 local and state law enforcement agencies in the United States use some form of CCTV surveillance technology in police operations including vehicles, bookings, public places, and "other police procedures."[44] According to the Chiefs of Police survey, most agencies particularly use CCTV cameras in police vehicles, inside or outside government buildings, or at special events.

The U.S. Office of Justice Assistance and the National Institute of Justice have been important funding sources for local projects through the Bryne Memorial Formula Grant Program, Local Crime Prevention Block Grant Program, and the Office of Science and Technology Program. A number of local jurisdictions have sought state funding or have collaborated with private sources to secure funding. In general, we find that there have been very few studies of the effectiveness of the CCTV surveillance systems. Crime-related statistical data are not required for use of federal grant funds, nor is there a requirement that all grantees report incidents of crime occurring where the cameras are located.

Despite their increasing use, there is limited evidence that CCTV camera surveillance programs are successful crime-prevention tools. According the International Association of Chiefs of Police survey, 96 percent of the responding law enforcement agencies using CCTV surveillance do not incorporate an evaluation component that measures the effectiveness of the system. Some law enforcement agencies have even discontinued the use of public CCTV surveillance. In 1999, the New York City police department removed CCTV cameras from strategic areas in the city after more than 18 months because they had resulted in only ten arrests. Nonetheless, more than 2,300 CCTV surveillance cameras remain in use in Manhattan, 85 percent of which are private. In Newark, New Jersey, an analog CCTV system set up in 1994 was discontinued in 2000 because of the staff time involved in monitoring the system. In Oakland, California, the city council withdrew a proposal to install a city CCTV surveillance system in 1997. Last year in Huntington Beach, California, an effort by the downtown business community to install CCTV surveillance cameras also failed.

SURVEY OF U.S. CITIES WITH CCTV CAMERA SURVEILLANCE SYSTEMS

Early this year, CRB undertook a telephone survey to identify public CCTV surveillance systems currently operating in the United States. Many are located in the eastern half of

the country, with the majority on the east coast. Some researchers believe this is because most eastern cities have higher density populations than in the west, which makes for easier surveillance. First we describe CCTV systems in other parts of the country, and then we discuss California. Table 1 summarizes our findings for the rest of the country.

Table 1
U.S. Cities (not including California) Using CCTV Public Surveillance Cameras

City/Town	Installation Date	Site Location	Funding Source	Reason For Use	Time of Operation	Type of Surveillance
Baltimore, MD	June 1996	Downtown	Private/Public	Drugs and street crime	7 a.m. to 11 p.m.	Active monitoring
Dover, NJ	September 1993	Downtown	Federal funds	Loitering	Around the clock	Active monitoring
Jersey City, NJ	2000	Citywide	Federal grants	Street crime	7 a.m. to 11 p.m.	Active monitoring
South Orange, NJ	1994	City parking lots and streets	Federal and city	Crime prevention	Daytime hours	Active monitoring
Charleston, SC	1997	Citywide	Federal/state	Street crime	Around the clock	Active monitoring
Tukwila, WA	August 1995	Business district	City funds	Drugs and Prostitution	Around the clock	Active monitoring
Federal Way, WA	2001	Downtown	Federal funds	Drugs and Prostitution	Around he clock	Active monitoring
Tacoma, WA	August 1993	Hilltop district	City funds	Drugs and Prostitution	Around the clock	Active monitoring
Tampa/St. Pete, FL*	September 1996	Ybor City	Public/private	Crime prevention	Around the clock	Active monitoring
Virginia Beach, VA*	2000	Waterfront district	City/private	Crime prevention	6 a.m. to 7 p.m.	Active monitoring
Anchorage, AK	1992	Entertainment district	State/private	Drugs and prostitution	7 p.m. to 4 a.m.	Passive monitoring
Memphis, TN	1996	Downtown	State/private	Crime prevention	Around the clock	Active monitoring
Gulfport, MS	2000	Business District	Private/public	Crime prevention	Daytime hours	Active monitoring
Nevada, MO	2001	City Parklands	Private funds	Petty crime prevention	Around the clock	Active monitoring
New Orleans, LA	1998	Entertainment district	Private/public	Crime prevention	Around the clock	Active monitoring
Cleveland, OH	1997	Entertainment district	Private funds	Crime prevention	7 p.m. to 2 a.m.	Passive monitoring
Honolulu, HI	1998	Chinatown area	City funds	Crime and Prostitution	Around the clock	Active monitoring

Source: California Research Bureau telephone survey and literature review, 2002
* Indicates use of biometric facial recognition technology in conjunction with CCTV

- *Washington D.C.* has established the most extensive public CCTV surveillance system in the country, linking hundreds of cameras that monitor mass transit stations, monuments and schools with new digital cameras that watch over streets, shopping areas and neighborhoods.[45]

- *Baltimore:* In September 1995, the Baltimore Police Department, the Downtown Partnership of Baltimore and the Mass Transit Authority jointly applied for and received a $75,000 Byrne Memorial federal grant to implement a "Video Patrol Project." The project was based on the concern that the downtown business district would continue to decline and fail to attract consumers unless crime (and the fear of crime) was effectively addressed. Aggressive panhandling, prostitution, street dealing of drugs, and larcenies from vehicles were the most notable crimes.[46]

- *New Jersey*: The cities of Jersey City, South Orange, and Dover all employ CCTV surveillance systems. In 1994, South Orange approved the installation of seven CCTV surveillance cameras to promote public safety in parking lots, intersections, and parks. The project cost $10,000 and was funded through a combination of federal grants and municipal funds. Jersey City began using CCTV surveillance in 2000 in its downtown core area. In Dover Township, the city recently installed a digital CCTV system to monitor activity on two high school campuses, several street intersections and the downtown mall area. It is the first time that a coordinated effort to link three different venues at the same time has been undertaken.[47]

- *St. Petersburg\Tampa Bay:* CCTV surveillance equipment was purchased by the city in 1995 to promote safety in the growing suburban business and entertainment district known as Ybor City (a pedestrian mall). This two-by-ten square block area has many clubs, restaurants, and some shops. According to a Tampa Bay Police Department spokesperson, CCTV surveillance is the "way of the future" to meet the growing security needs of entertainment districts that attract large crowds.[48]

  In early 2001, the police added biometric technology to the CCTV surveillance system in order to scan the faces of people videotaped in the Ybor City district, as had recently been done at the Super Bowl. The upgraded surveillance system snapped pictures of faces and compared them with 30,000 images in a database that included runaways and wanted criminals. However, the biometric scanning system was recently discontinued because of public concern over its reliability and its limited success as a crime prevention tool. [49]

- *Virginia Beach:* Virginia Beach began a CCTV video surveillance program in 1993, with support from the public, business, and the police. CCTV video cameras cover 27 blocks of beachfront area, and are mounted on existing signal devices and street light poles, and are enclosed in weatherproof spheres with tinted domes.[50] The city later added a biometric component to the system. It is the only city in the country currently using biometric face recognition technology in conjunction with a CCTV surveillance system.

- *Memphis*: In 1996, Memphis undertook a $450,000 CCTV video surveillance program for the downtown business and entertainment district to discourage and prevent crime. The CCTV system consists of ten pan-and-tilt zoom cameras mounted on buildings covering a 12-square-block area known as the Pinch District. The CCTV cameras are linked to a police dispatch center via a fiber optic cable. Volunteers and police continuously monitor the CCTV system.[51]

- *Anchorage, Alaska***:** Anchorage has seven mobile community patrols that videotape any illegal activity within an assigned neighborhood and transfer the digitized images to a central location via the Internet. This volunteer video patrol effort began in 1992 as a way to help the middle-class neighborhood of Spenard rid itself of gambling and prostitution. The tapes are edited for clarity until a perpetrator is identified, and the image is then printed on paper and passed on to the police or to local businesses. Funding for the video patrols comes from the business community and state grants.[52]

- *Washington State:* The cities of Tacoma, Tukwila, and Federal Way all have CCTV surveillance programs.[†] Tacoma was one of the first cities to install a CCTV video surveillance system to tackle neighborhood crime, and the system is still operating. Crimes detectable by cameras, such as assaults, trespassing, prostitution and vandalism, decreased from 244 incidents in 1993 to 87 incidents in 1994. In 1995, the number of crimes increased to 125, still less than half the number reported in 1993.[53]

  Tukwila started its eight-block CCTV surveillance system because street thugs were robbing unsuspecting pedestrians by day and prostitutes were operating by night. Police and specially trained volunteers monitor this area day and night from a centrally located storefront.

  Federal Way is a small city in the Seattle area that received a federal grant of $96,000 to install CCTV surveillance cameras in the downtown core area. The surveillance program went into effect in August 2001, with the goal of helping law enforcement to reduce drug sales and prostitution activity along the Pacific Coast area of downtown.

- *Nevada, Missouri:* Ten CCTV surveillance cameras cover the town's 14,000 square foot community center in order to improve security. This small town faces some of the same public safety problems as big cities, according to the Parks and Recreation Director.[54]

- *Charleston, South Carolina*: CCTV surveillance cameras were first installed in 1997 and have since expanded throughout the city's downtown business district. The cameras are monitored and operated by the police department, and the

[†] Urban communities in the greater Seattle area are also using CCTV surveillance cameras in their downtown and major business areas.

program is supported by businesses and by crime victims. Other communities near Charleston are considering similar surveillance programs.[55]

CALIFORNIA CITIES WITH CCTV VIDEO SURVEILLANCE

According to a spokesperson for the League of California Cities, it is not a common practice for California police departments and cities to use CCTV cameras to monitor public areas in their jurisdictions.[56] In contrast, many local public agencies (such as libraries, public housing, and parks and recreation departments) deploy CCTV surveillance cameras, but their function is primarily to protect property rather than to monitor public movement. Cities and state agencies are becoming increasingly vigilant in protecting public buildings by installing CCTV surveillance cameras. Table 2 briefly describes public CCTV surveillance programs in California (there may be other examples our survey did not locate), with more detailed information presented for several cities.

- *San Diego*: The San Diego CCTV surveillance program that began in 1993 is unlike other camera surveillance programs in that it is used on behalf of the city's park system, which is the heart of its tourism industry. The Balboa Park CCTV system consists of five cameras that monitor the area's pedestrian mall and museum buildings. The system was funded by the private sector. It is currently off-line for upgrading. When operational, the CCTV system films continuously, but the video images are actively monitored only during regular business hours.[57]

- *Hollywood:* In 1995, building owners and landlords in the Yucca Street corridor collectively pooled their resources ($15,000) to purchase and install CCTV cameras atop apartment buildings and business entrances. According to a police spokesperson, the effort was successful in discouraging potential crime. However by 1999, the system had become antiquated by modern technology standards and was deactivated. Today, a new effort is underway by local community leaders and the Hollywood Division of the Los Angeles Police Department to purchase and install a state of the art digital CCTV camera system that would be easy for volunteers and the police to operate and monitor. There is broad support in the community for this new effort. It is anticipated that funds for a new system will be from a combination of local, state, federal and private sources.[58]

- *Palms Springs*: In June 2001, the Palm Springs City Council received a state technology grant and a federal justice assistance grant to purchase CCTV surveillance cameras. The system of 14 cameras will monitor a half-mile stretch of Palm Canyon Drive in the downtown area. The camera system will be passively monitored by dispatchers as time permits, and all tapes will be reviewed before they are erased. According to City Manager, David Ready, "the idea is to give people a higher level of security so they can enjoy themselves. The reality is we can't afford to put an officer on every corner."[59]

- *Vallejo:* In November 2000, the Vallejo City Council approved the installation of CCTV surveillance cameras, along with the hiring of two community policing officers, to monitor crime activity in the downtown area of the city. The purchase of the camera surveillance system was funded by local general funds. According to a police spokesperson, the system will be operational in February 2002.[60]

CCTV Surveillance camera in front of California's State Capitol located in Sacramento.

Table 2 Cities in California And Use of CCTV Public Surveillance Programs			
City	**CCTV Surveillance System**	**Location of System**	**Future Consideration**
Sacramento	Yes-privately operated and monitored by the downtown merchants association.	Downtown business district	None
San Francisco	Yes-to reduce criminal activity on buses.	Various Muni buses and rail system trains.	Yes-as funds become available
Oakland	No-rejected in 1997	Was proposed for the downtown area.	Yes-the Oakland International Airport
San Jose-Silicon Valley	Yes	Commercial district	Yes
Vallejo	Yes-to discourage crime	Downtown	Yes
Los Angeles	Discontinued in 1999 in the Hollywood area of Los Angeles.	Yucca Street corridor	Yes-a digital system is in the planning stages
Lakewood	Discontinued in 2000 after two year project to address graffiti and gang activity	Residential neighborhoods	Yes-as the need for this type of surveillance is warranted
Palm Springs	Yes	Business district	Yes
San Diego	Yes	Balboa Park	Yes

Source: California Research Bureau Survey, 2002

Red Light Camera Surveillance

According to data from the National Highway Traffic Safety Administration, there were about 6.3 million reported crashes on U.S. roadways in 2000. Approximately 40 percent of those motor vehicle crashes occurred at intersections or were intersection-related.[61] Since 1992, the Federal Highway Administration has spent millions of dollars promoting photo enforcement systems at intersections (red light surveillance cameras) and helping local jurisdictions to install them. Red light cameras automatically photograph vehicles whose drivers run red lights.

The nature and operation of red light camera programs are determined by state and local law enforcement as well as by elected officials. While there is some variation from state to state, most systems operate and work in the following manner:

- Local engineers determine the timing at traffic signals, including the length of the green, yellow, and red phases.
- A red light camera system is connected to a traffic signal and sensors buried in the pavement at a crosswalk or stop sign.
- In most cases, the system monitors the traffic signal and triggers the camera to photograph the tags of vehicles entering the intersection after the light has turned red.
- The camera is triggered by any vehicle passing over the sensors above a pre-set minimum speed and at a specified time after the signal has turned red.
- The camera records the date, time, and speed of the vehicle, and a clear image is produced (under a wide range of light and weather conditions).

At least 60 communities in the U.S. are using red light surveillance cameras, including large cities like New York and Los Angeles. California, Maryland and Hawaii have by far the most red light cameras (see Table 3 below).[62] Currently, five states (Alaska, Nebraska, New Jersey, Utah, and Wisconsin) have banned photo enforcement systems.

Table 3
Cities in States With Red Light Camera Surveillance Programs

Arizona	Colorado	Virginia
Chandler	Boulder	Alexandria
Mesa	Denver	Arlington
Paradise Valley	Fort Collins	Fairfax City
Phoenix		Fairfax County
Scottsdale		Falls Church
Temple		Vienna

California		Maryland		North Carolina
Beverly Hills	Redwood City	Anne Arundel County		Charlotte
Culver City	Sacramento City	Annapolis	Howard County	Fayetteville
Cupertino	Sacramento County	Baltimore	Hyattsville	Greensboro
El Cajon	San Buenaventura	Baltimore County	Laurel	High Point
Fremont	San Diego	Bel Air	Landover Hills	Willington
Garden Grove	San Francisco	Blandensburg	Montgomery County	
Indian Wells	San Juan Capistrano	Charles County	Morningside	
Irvine	Santa Rosa	Cheverly	Prince George County	
Long Beach	West Hollywood	Cottage City	Riverdale Park	
Los Angeles City	Ventura	Forest Heights		
Los Angeles County	Oxnard	Greenbelt		

Delaware	District of Columbia	Ohio
Wilmington	Washington D.C.	Toledo

Hawaii (statewide)	New York	Oregon
	New York City	Beaverton
		Portland

Washington		
Lakewood		

Source: Insurance Institute for Highway Safety, Highway Loss Data Institute, 2001

In Washington, D.C., the police department reports that their red light surveillance program resulted in a 63 percent reduction in red light runners at 39 intersections in the first year of operation, and a decrease in fatalities as well.[63] A 1999 Insurance Institute for Highway Safety study in Oxnard, California, found that red light running violations dropped a total of 42 percent within a year after photo enforcement was introduced.[64] Another study in Fairfax, Virginia, showed that red light violations declined 40 percent after one year of photo enforcement.[65] In San Francisco, the police department began using a red light surveillance program to monitor vehicle traffic in 1996. According to a police department spokesperson, the surveillance program was prompted in part by public demand to crack down on "speeders" who consistently run red lights and endanger other vehicles and pedestrians. Within six months after the program began, red light running was reduced by nearly 40 percent.[66] The public generally seems to support local adoption of red light running photo-enforcement laws, with a Harris Poll finding 69 percent public support.[67]

Recent Congressional testimony questions the effectiveness of red light systems.[68] Technical criticism relates to the inconsistencies in the way traffic engineers change timing standards to accommodate camera enforcement. Individual traffic signals are not timed in a consistent manner, particularly as to the length of yellow lights.[69] According to the Insurance Institute for Highway Safety, yellow lights must be timed to accommodate a wide range of circumstances. As a result, the Institute of Transportation Engineers (ITE) and Federal Highway Administration provide guidance to local traffic engineers on signal timing using two different approaches. Engineers can either employ a uniform value for the length of yellow change intervals, or set the timing for each intersection individually to take into account factors such as geometry and traffic speeds.[70]

Critics of the programs contend that they are merely a way to generate more tax revenue. For example, New York officials report that they have collected an average of $8.5 million per year since the city's red light surveillance system was installed. In San Diego, a judge dismissed nearly 300 tickets in a class-action lawsuit, ruling that the evidence was unreliable because the system is privately run and the company is paid through a percentage of the fines. Also, there may actually have been an increase in accidents in San Diego intersections as people brake to avoid the costly fine.

Public and Regional Transit

Public transit systems across the country have installed video cameras in buses and rail stations for reasons including crime prevention and response, risk management, legal evidence, responses to events in progress, customer service, and employee security. Municipal bus systems in Portland, San Francisco, and Cleveland use video cameras mounted on top of buses to record passenger activity in and out of buses. Municipal bus systems in Philadelphia, Chicago, and San Antonio use video surveillance cameras inside of buses to help prevent fraudulent injury claims and reduce incidents of passenger harassment and property damage.[71]

CCTV surveillance cameras are also used by municipal rails systems in California. For example, the San Francisco County Board of Supervisors received a $2 million state grant in 2000 to install digital CCTV surveillance cameras on Municipal Railway transit vehicles.[72] The Bay Area Regional Transit (BART) system uses CCTV surveillance cameras in major rail stations all along the entire BART line. In Los Angeles and Sacramento CCTV cameras are used on certain rail lines that have demonstrated high crime rates.

According to a national transit survey conducted in 2001, 26 transit agencies reported using surveillance systems in their operations. Most transit agencies responding to the survey make full use of their CCTV systems by continuously monitoring passenger activity inside buses; a smaller number use surveillance systems only to record events, and; a few use audio surveillance. According to the survey, few, if any, transit systems use CCTV cameras on their entire fleet of buses or in all facilities. Most commonly (11 of 26 agencies), respondents reported that less than 25 percent of their agency's fleet is

equipped with surveillance cameras. Most agencies install CCTV cameras in response to specific crime, fraud, disorder, safety, or passenger complaints on certain routes. [73] Concerns over the lack of disclosure about surveillance systems on buses have led most transit agencies to inform riders about the CCTV cameras. According to the National Transportation Research Board, signs should be posted in all vehicles and premises notifying the public of the cameras and that information is being gathered and recorded via the surveillance system. The National Research Council advises that if signs are present alerting the public that surveillance is being used, this constitutes a legal obligation by the transit agency (in some instances) to perform such surveillance. The nature of the obligation differs from state to state.[74]

Table 4 presents a brief description of the cities with transit districts using CCTV systems.

Table 4
Transit Systems in the United States Using CCTV Camera Surveillance Systems

Name of City/Area	Transit System	Type of Surveillance	Date	Results
Ann Arbor, MI	Bus system	Digital CCTV	1997	Improved perception of security
Bakersfield, CA	Bus system	Analog CCTV	1997	N/A
BART, CA	Rail Stations	Digital CCTV	1999	N/A
Buffalo, NY	Bus system	Digital CCTV	1995	Anecdotal evidence-System is effective
Chicago, IL	Bus system	Digital CCTV	1996	Limited arrests
Cleveland, OH	Bus system	Digital CCTV	1996	N/A
Columbus, OH	Bus system	Digital CCTV	1997	Improved perception of security
Coupeville, WA	Bus system	Analog CCTV/audio	1999	N/A
Denver, CO	Bus system	Digital CCTV	1997	N/A
Durango, CO	Bus/trolley system	Analog CCTV	2001	N/A
Houston, TX	Bus system	Digital CCTV	2001	Improved perception of security
Lancaster, CA	Bus system	Digital CCTV	1998	N/A
Los Angeles, CA	Bus and rail systems	Digital CCTV	1995	N/A
Milwaukee, WI	Bus system	Digital CCTV	1999	Improved perception of security
Oakland, CA	Bus system	Digital CCTV	1999	Improved perception of security
Philadelphia, PA	Bus system	Digital/Analog CCTV	1993	Improved perception of security
Portland, OR	Bus and light rail systems	Digital and Analog CCTV	1987	Vandalism is down
San Antonio, TX	Bus system	Digital CCTV	2001	N/A
San Francisco, CA	Bus and rail systems	Digital CCTV	1996	Improved perception of security
Seattle, WA	Bus system	Digital CCTV	1996	N/A
St. Louis, MO	Light rail system	Digital and analog CCTV	1997	Complaint reduction
Tampa Bay, FL	Bus system	Digital CCTV	2000	Improved perception of security
Thousand Palms, CA	Bus system	Digital CCTV	1999	N/A
Torrance, CA	Bus system	Analog CCTV	1998	N/A
Washington, DC	Bus system	Digital CCTV	1998	N/A

Source: California Research Bureau, 2002

The California Department of Transportation (CalTrans) utilizes video cameras on many of the state's major freeway systems to monitor and regulate traffic flow. CalTrans also uses an "Automatic Vehicle Identification" system for road tolls, which identifies cars as they pass roadside sensors at toll plazas. Transponders located in license plates and pass cards identify a car's registrant via roadside sensors, which in turn trigger deductions from road user accounts.[75] Other toll road systems in Florida and in New Jersey use CCTV surveillance cameras to identify moving violators and prevent car hold-ups.

Amtrak uses an "interactive video" system (PFA Flex 300) at major rail stations in Chicago, New York, and Washington for information and ticketing, and for agent and client interface. According to an Amtrak spokesperson, the interactive system allows potential passengers and live agents located at a remote station or location to conduct business. This system allows agents to combine the needs of low-volume stations with other tasks. The PFA Flex 300 is being tested for CCTV video surveillance, public announcements, environmental control of temperature, lighting and door locking, infrared sensors, credit card reading capability, and train status information.[76]

CCTV PROGRAMS IN PUBLIC HOUSING

In the United States, there are approximately 4.8 million public housing units ranging in size from one to a 1,000 units; 60 percent are relatively small, with one to 49 units. Eleven out of the fifteen largest public housing projects are located in the eastern half of the country.[77]

Neighborhood activists and police have teamed up over the past several years to address local crime concerns by incorporating video surveillance with other crime prevention measures in public housing projects. CCTV camera systems are becoming a major part of new *place-specific crime prevention* strategies employed by housing administrators. Various examples of this new security approach call for physical design and management changes, including enhanced security, improved property management, and greater residential involvement.[78]

- In *Richmond, Virginia,* a housing project for 200 families received HUD funding and community oriented police (COP) funding for police patrols and digital CCTV surveillance cameras.[79]

- In the *Boston* public housing projects of Roxie Homes, Camfield Gardens, and Grant Manor, a major collaborative effort was recently undertaken to improve the quality of life. Trained security officers from the projects, who have arresting powers, monitor the CCTV camera from within the project and respond to any illegal activity captured on the video. The project, known as Safe Neighborhood Action Plan (SNAP), cost $1.3 million to implement and has reduced crime in the three projects by 30 percent.[80]

Most public housing projects are managed by local governmental agencies. Numerous housing projects are privately owned and financed with government mortgages via local

housing finance agencies. The vast majority of these housing units are for low-income families and individuals living on government subsistence.[81] In Massachusetts, the housing finance authority (MHFA) spends $3 million annually on security for 9,000 units throughout the state.[82] There are other government funding sources available for local applicants, including community oriented policing and justice assistance grants from the U.S. Department of Justice, and U.S. Department of Housing and Urban Development (HUD) grants. Information about public housing project security and safety requirements is not collected by any federal or state agency. However, managers and operators of federally funded public housing are required to conduct an annual Public Housing Assessment Security Survey (PHASS) of tenants to determine consumer satisfaction.

CALIFORNIA'S PUBLIC HOUSING CCTV PROGRAMS

The California Department of Community Housing and Development administers funding for public housing projects in California. According to department officials, public housing agreements with local housing officials do not require stipulations for reasonable expenditures on security measures. The state also does not collect crime-specific data about state funded public housing programs, whether they are privately or publicly managed. According to representatives of the nonprofit Housing Association of Northern and Southern California (representing private owners and investors of public housing), no security stipulations are required in any of the contracts they sign. While these privately owned housing units are reserved for low-income families and individuals living on government subsistence, it is the responsibility of the housing managers to pay for on-site security measures.

Anecdotal information suggests that many of the estimated 130,000 public housing units in the state are monitored by private security personnel or are patrolled by local police departments as part of a community policing program. Larger projects with 300 or more housing units are more likely to use CCTV surveillance cameras. Most of the large housing projects in California (high-rise buildings or large two-story housing complexes) are located in San Francisco, Oakland, and Los Angeles. While the exact number of housing units in these cities using CCTV surveillance is unknown, CCTV surveillance cameras are a major component of security, according to a public housing official interviewed for this report.[83] CCTV surveillance cameras also play a major role in security in public and privately funded senior housing projects across the state.[84]

Even in rural areas, such as Eureka and Porterville, public housing projects are using CCTV surveillance cameras as the primary source of security.

- In *Porterville,* the local housing authority installed six CCTV cameras in a ten-story elderly public housing project with the help of federal and state funds in December 2001. The CCTV cameras are mounted on street poles and monitor activity in and around the entrances to the building.[85]

- In *Eureka,* the local housing authority installed seven CCTV surveillance cameras in a multi-family housing project in 2001. The project was funded through a

federal grant and is required to keep statistical data about crime occurring where the cameras are located.[86]

CCTV SURVEILLANCE SYSTEMS IN SCHOOLS

School districts across the country began using CCTV surveillance systems in the mid-1990s, before a wave of tragic school shootings. Some district administrators now believe that CCTV cameras are an essential part of crime prevention in schools. When asked whether an effective CCTV surveillance system could have prevented the Columbine killings, a Huntsville, Alabama, school district official said "probably not, but it could have minimized the damage."[87]

Benefits ascribed to school CCTV surveillance systems include:

- Gives both students and faculty "peace of mind" and a sense of safety
- Provides a "deterrence factor" to outsiders who do not belong on campus and to students and employees who do
- Provides school administrators or security personnel with information not otherwise available, i.e., evidence can be preserved on tape
- Frees up manpower for more appropriate work
- Performs mundane tasks and saves money[88]

Video surveillance cameras target the following school security concerns:

- Outsiders on campus
- Fights on campus
- Theft
- Parking lot problems
- Bus problems
- Teacher safety[89]

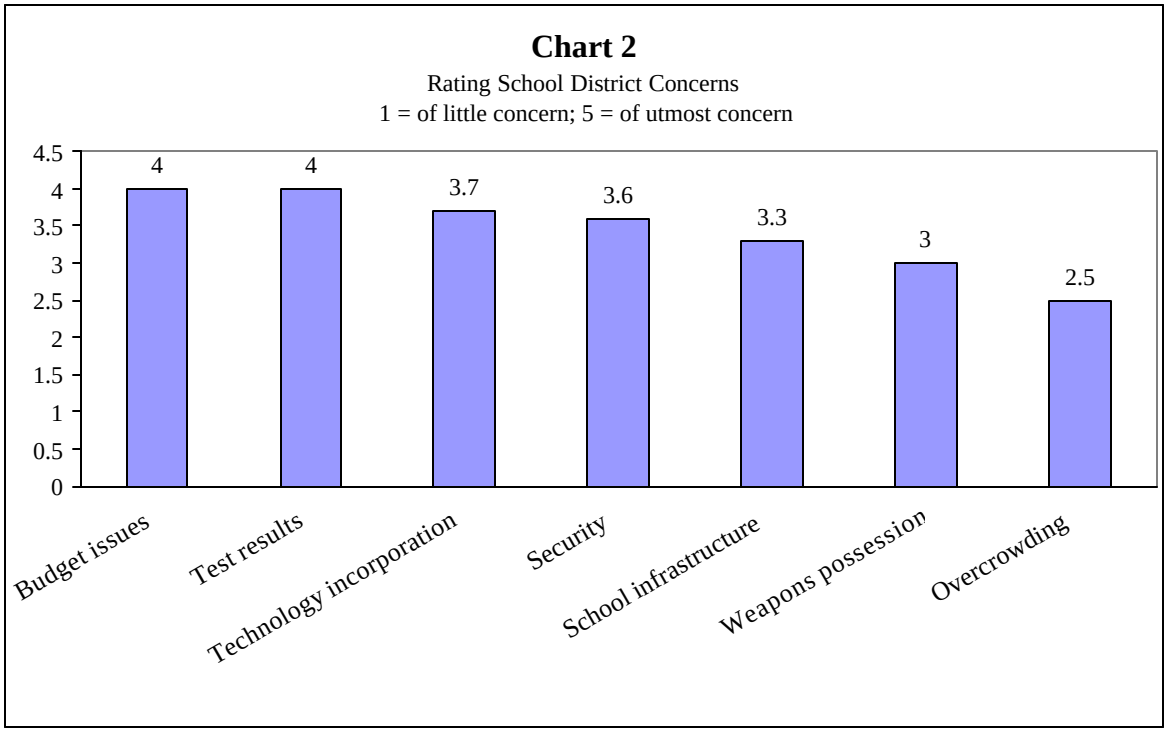
Some school districts have invested heavily in CCTV surveillance technology. For example, nearly all of the 98 public schools in Atlanta, Georgia have installed high-tech surveillance equipment. The cost of installation and equipment was $3.3 million.[90] There are substantial additional costs over time for maintenance and personnel. Given the cost, school security consultants advise school officials to evaluate the following questions prior to committing community resources for school video surveillance systems:

- What specific security threats are you attempting to address?
- How will the equipment help address these threats?
- If you are able to purchase the equipment, who will use it, how will it be used, and how will it be maintained and repaired?[91]

By themselves, security technologies such as video surveillance may offer only a "quick fix, aggressively marketed, and something tangible that administrators can show to their community as their way of securing school premises."[92] School administrators may also face a basic paradox: the more obtrusive security equipment a school contains, the less safe it feels.[93]

A 2000 national survey of school administrators, conducted by American School & University (AS&U), highlights school security practices and concerns.[94] Some of the key survey findings include: ‡

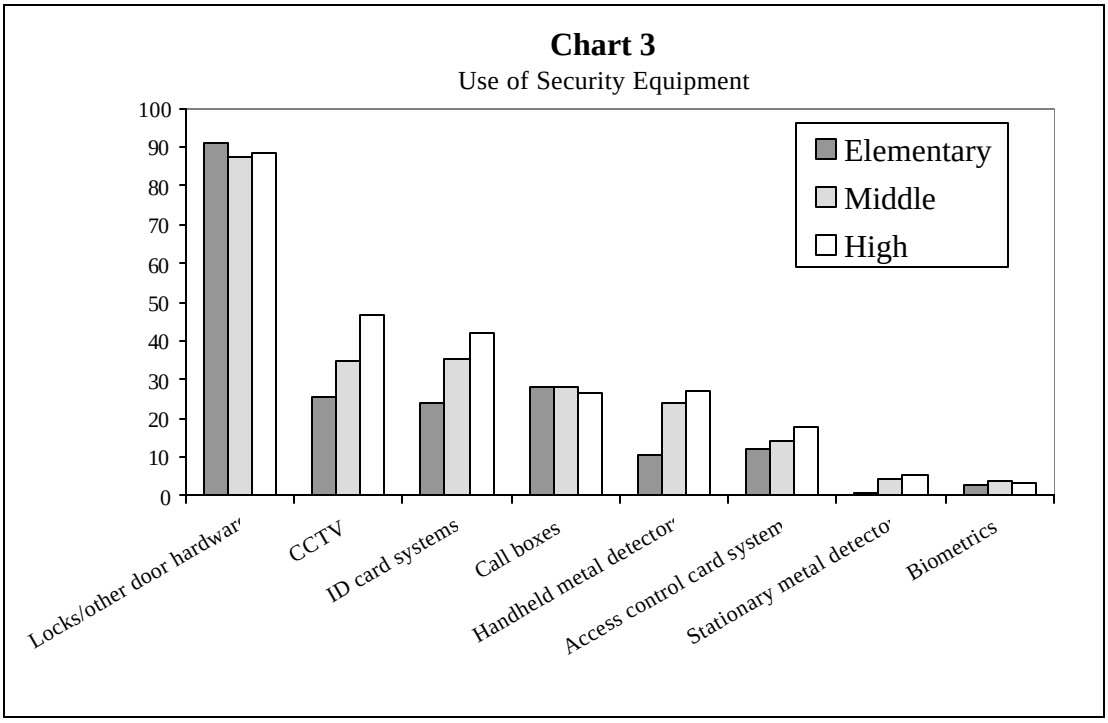
- 70 percent of the school officials rated security issues as being of utmost importance in creating an environment conducive to learning (an average 4.5 rating on a scale of 1 to 5, with 5 being of utmost importance)
- Security was one of the top four concerns of the respondents, as shown in Chart 2 below.
- A number of factors influence school security decisions, ranging from strategic planning to pressures from constituents.



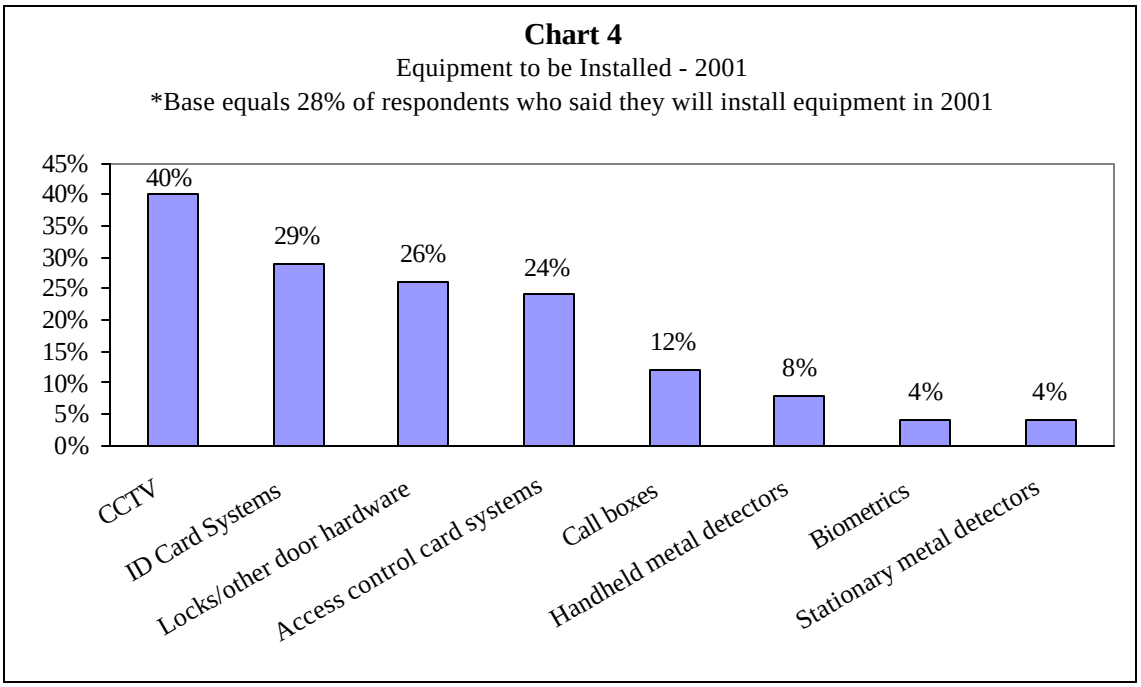
Source: *AS&U* School Security Survey, 2000

‡ The survey was based on 439 telephone interviews. The average student enrollment of the respondents' districts was 5,029 students. One-third of the districts had less than 1,000 students, 29 percent had 1,000 to 2,499 students, 22 percent had 2,500 to 9,999 students, and 14 percent had more than 10,000 students.

Low technology locks are still the most common security equipment in elementary, middle and high schools. However, at the high school level CCTV video surveillance is the second most common security equipment. Further, CCTV, handheld metal detectors and ID card systems are increasingly being installed in elementary school districts that have a lot of buildings (See Chart 3).[95] CCTV was the most common security system that districts planned to install in 2001 (See Chart 4).



Source: *AS & U* School Security Survey, 2000



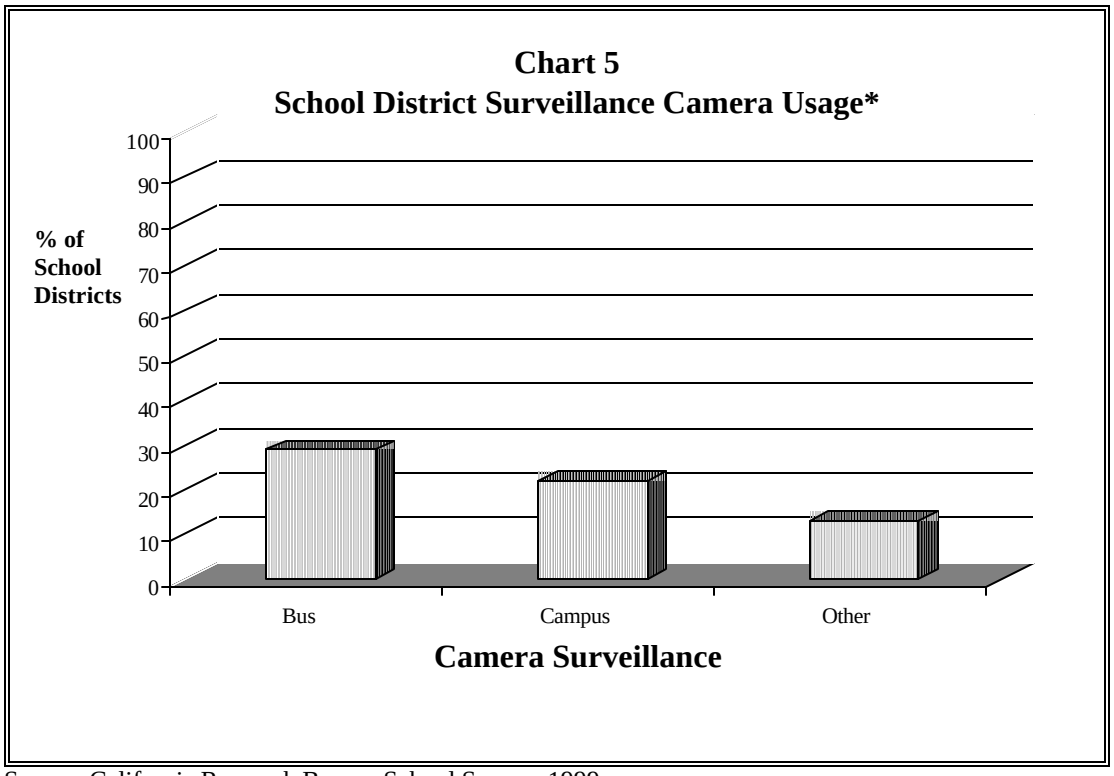
Source: *AS&U* School Security Survey, 2000

SECURITY TECHNOLOGIES IN CALIFORNIA SCHOOLS

In 1999, the California Research Bureau conducted a statewide survey to assess the security measures and crime prevention resources used in California school districts.[96] At that time, many California school districts were incorporating closed circuit video surveillance (CCTV) into their school safety programs. According to the 1999 CRB school survey:

- 29 percent of school districts used CCTV cameras on school buses
- 22 percent of the districts placed CCTV cameras on campuses
- 13 percent used CCTV cameras to monitor other school property

These figures are an impressive increase from 1996, when a CRB study found that only a few school districts in California had placed CCTV surveillance cameras on campus.[97]



Source: California Research Bureau School Survey, 1999
*Sixty-five school districts reported using camera surveillance

The *California Safe Schools Act* of 2000 allowed school districts to use state grant funds to purchase CCTV equipment. Examples of installations last year, in both middle and high schools, include the Huntington Beach, Colton and Moreno Valley school districts.

- In Huntington Beach, surveillance cameras were recently installed as a pilot project in one high school to deter vandalism, at the request of the district's insurance carrier. The insurance carrier is paying for the pilot program equipment, and the district will pay for any cameras installed in other schools. The cameras are only used to record incidents and are not connected to a monitoring system. If the district finds that the pilot system is effective in deterring vandalism, surveillance equipment will be installed throughout the district within a year.[98]

- In Moreno Valley, surveillance cameras have been installed in one high school as a pilot program, using state funds. If the pilot program is successful, cameras will be installed in other Moreno Valley high schools. The surveillance system has no monitoring capability and only records incidents.[99]

- All the middle and high schools in the Colton Valley school district installed video surveillance systems in the past year, with funding from a $550,000 state grant awarded through the Safe Schools and Violence Prevention Program. The system has an active monitoring capability that can be accessed through the Internet. It will be monitored by principals, assistant principals and selected district officials.[100]

BUSINESS AND WORKPLACE APPLICATIONS OF CCTV SURVEILLANCE

Video surveillance in America is not a recent phenomenon. Businesses began using CCTV surveillance in the early 1960s, first in banks, as mandated by federal banking law, and later in commercial buildings. In the 1970s, CCTV surveillance was deployed in hospitals, all-night convenience stores, art galleries, and in many other commercial areas. Video technology was limited to *passively* recording events, with little or no means for remote monitoring. Picture quality was often poor. For example, on many occasions police officials were unable to prosecute criminals caught in the act by remote video cameras because quick movements resulted in *low quality* pictures.[101]

Video technology advanced during the1980s with the introduction of camcorder technology, and even more in the 1990s with digital technology, improved camera coverage, and weather resistant housing. Private sector uses included industry/manufacturing, retailing, transportation and distribution, banking, utilities, and hotels/motels. Many businesses invested heavily in video surveillance technology as a means to protect products and to promote safe environments. By 1997, web-based digital and computer technology began emerging as a more effective means to improve the video image of analogue surveillance cameras and to interact with CCTV systems. Today many businesses are combining these two technologies to improve security. For example, CCTV cameras surveillance

Notice of CCTV surveillance in use.

systems used in concert with web-based Internet Protocol (IP) computers make it possible to transmit live video of any crime to any remote server over the Internet. IP surveillance systems transmit live video streams of up to 30 frames/second into a standard web

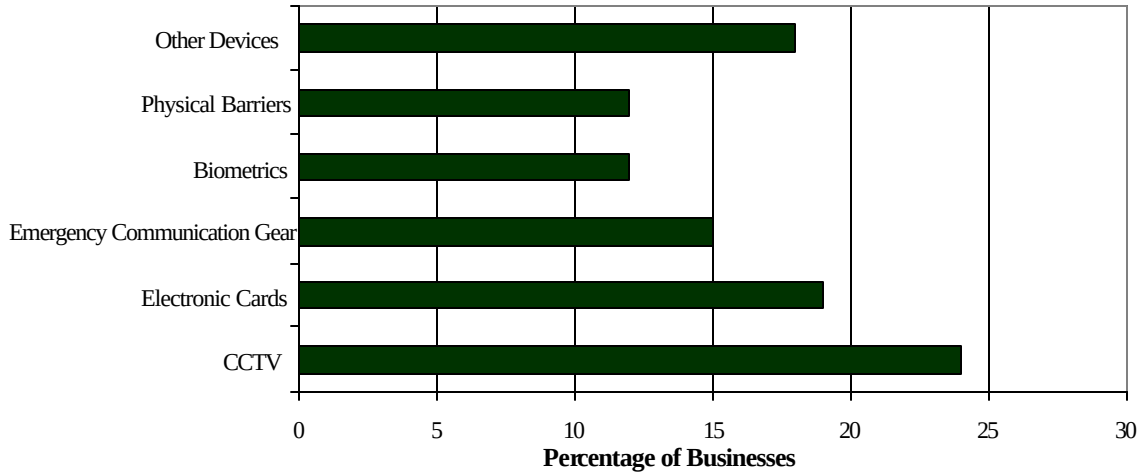
browser. Retail industry employees, especially those constantly exposed to the threat of armed robbery such as in convenience stores, are now monitored on the job from a central location by company security staff.[102]

AN EXPANDING SURVEILLANCE INDUSTRY

According to a national survey taken in October, 2001, shortly after the September 11 terrorist attacks, nearly 90 percent of American companies had taken actions to re-evaluate their security operations, upgrade or buy new security systems, or increased security staff. The survey asked companies to identify the type of security technology that would make the biggest difference in fighting terrorism. CCTV camera surveillance was the most frequently mentioned technology, followed by electronic card key access, and emergency communication gear (See Chart 6).[103] Over 50 percent of all CCTV surveillance sales involve industrial and commercial clients.

Chart 6

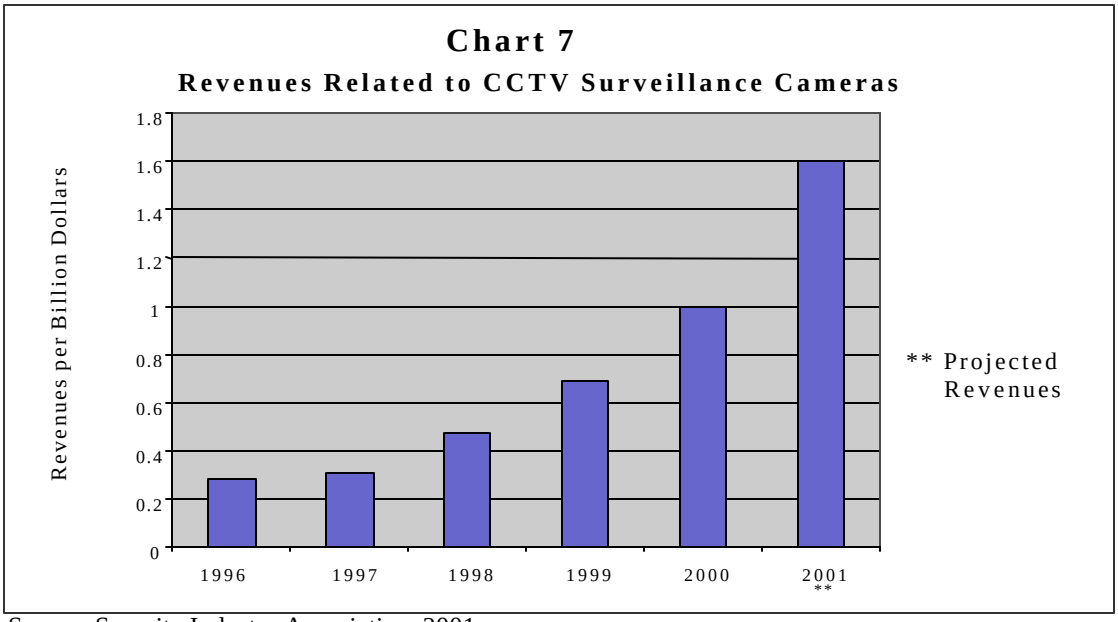
Survey of Security Options Favored By National and Worldwide Companies



Source: *Security Magazine Survey*, October 2001

Commercial sales of CCTV camera surveillance equipment are reaching record levels.[104] Since 1997, the sale of CCTV surveillance equipment has surpassed the sales of burglar and fire alarm systems. Overall, the electronic surveillance industry has grossed about $40 billion a year since 1998. Annual revenues from the sale of video surveillance cameras more than tripled from $282 million in 1990 to more than $1 billion in 2000.

The Security Industry Association forecast that sales could grow to over $1.6 billion by the end of 2001 (See Chart 7 Below). After the terrorist attacks on New York and Washington D.C., some industry officials predicted that the sale of CCTV surveillance cameras in the U.S. could soar to nearly $5.7 billion by the end of 2001.[105]



Source: Security Industry Association, 2001

Industry officials estimate that there about two million CCTV cameras used in the U.S. for public safety and for security purposes in offices, apartment buildings, garages, stores, banks and ATM machines, and restaurants.[106] There are also literally thousands of CCTV cameras used by federal, state, and local governments on highways, in tollbooths, at intersections, in buildings, train stations, airports, prisons and post offices.[107]

CCTV IN THE WORKPLACE

CCTV surveillance is common in the American workplace setting. According to the *Privacy Journal*, an employer, manager, board member, or supervisor can legally videotape employees using hidden cameras if they suspect wrongdoing.[108] Some businesses are turning to CCTV surveillance to protect against employee law suits and other related damages. In addition to CCTV, other types of surveillance include telephone monitoring, e-mail and voice mail monitoring, computer keystroke monitoring, Internet website monitoring, location tracking using employee badges, and satellite tracking.[109] A 1996 study of workplace monitoring calculated that at least 40 million American workers were subject to some form of electronic surveillance.[110] In the public sector, transit workers can be scrutinized by confidential investigators using video surveillance.

CCTV cameras are also being used in nursing homes and assisted living communities across the country by what some people call "granny cams." Advocates of granny cams

believe that they promote better safety and care, citing a case in Alaska where the daughter of an elderly resident had a camera installed after frequent complaints about her father's care. The video camera recorded the 87-year-old man, who suffered from Alzheimer's disease, as he was left unattended in a bathroom for over an hour. As a result, the state's long-term care ombudsman found that nursing home staff violated basic standards of care.[111]

Most nursing-home officials oppose the granny cams movement. They contend that the cameras invade the privacy of residents and add to the difficulty of finding employees in an industry that is already short-staffed. They are concerned that videos from the cameras will be used as evidence in the burgeoning number of cases being brought against nursing homes. (Litigation is expanding so rapidly that membership in the National Academy of Elder Law Attorneys has increased tenfold in the past decade.)[112]

Concerns about privacy intersect with CCTV surveillance in some companies. Bathrooms and changing rooms are particular locations of contention, as the following examples suggest. The general manager of the *Apalachicola Times* newspaper in Florida installed a hidden camera in the employee bathroom to ensure that nothing illegal was happening. The management of the Boston Sheraton Hotel video recorded workers as they changed clothes in a locker room on the pretext of investigating suspected drug use by workers.[113] In 1997, hidden CCTV surveillance cameras were found in a men's bathroom of a trucking company in Riverside, California. After sheriff's deputies seized the CCTV cameras, a company spokesman said the equipment was installed to root out illegal activity and not to spy on people. Employees caught on tape sued the company for invasion of privacy in the 9th U.S. Court of Appeals. In September 2001, the court ruled that employees had the right to sue for invasion of privacy.[114] The 9th Circuit has also affirmed that federal labor law protects unionized workers engaged in picketing and organizing activities from video surveillance by employers.[115]

CCTV AND RETAIL SECURITY

American workers, especially those exposed to the threat of armed robbery, may feel increasingly safe in the presence of security equipment.[116] Recent research conducted by the National Association of Convenience Stores (NACS) studied the effectiveness of having two clerks present as a way to discourage crime and reduce injury. The study found that two clerks on duty, particularly during the night shift, had a positive effect by reducing the robbery rate in previously robbed stores. There was also some evidence that CCTV surveillance cameras with a monitor in the front, where potential perpetrators and others can see themselves, may show promise as a robbery deterrent.[117] However, researchers for the NACS conclude that while CCTV surveillance and video systems have become more prevalent in recent years, more focused research needs to be conducted in order to prove if CCTV cameras are effective.[118]

In 1995, the California Occupational Safety and Health Administration (*Cal/OSHA*) developed a model set of guidelines to reduce workplace injury, illness, and violence.[119] The guidelines create three categories of injury prevention. *Type 1* focuses on the

prevention of an external assault or threat by an outside third party. The *Type 1* guidelines recommend the following physical changes to business establishments in order to reduce violence (in rank order):

- Visibility
- Lighting
- Mirrors
- CCTV Cameras

Retail customers are increasingly comfortable with CCTV surveillance. A security industry official contends that, "years ago shoppers objected to electronic eyes recording their moves; today it's not only accepted, it's preferred."[120] This expectation raises liability issues for property owners. Courts have decided successful tort claims of negligent security involving video surveillance, brought by crime victims. Some cases claimed that owners did not provide adequate video surveillance to protect patrons or tenants. Other cases claimed that owners decreased security by replacing security guards with video surveillance.[121]

Legal and Privacy Issues Related to CCTV and Other Surveillance Technologies

> *The question we confront today is what limits there are upon this power of [surveillance] technology to shrink the realm of guaranteed privacy.*
> --Justice Antonin Scalia[122]

For three decades, most U.S. legal scholars agreed that continuous CCTV video surveillance of public areas did not present significant legal obstacles. This was because until the late 1990s, continuous video surveillance was mainly considered by courts and legislators to be a form of "passive" surveillance, comparable to a mechanical police officer. Thus, such use was not considered to be an intrusion upon an individual's privacy.[§]

Within the last five years however, four phenomena have significantly impacted the current and future legal debate regarding the appropriate use of video and related surveillance technologies and their implications for privacy rights.

1) The increasing capabilities and widespread use of law enforcement video surveillance technologies have become ubiquitous and sophisticated.
2) Civilian use has outpaced legal debate and proposed legislation.
3) A recent U.S. Supreme Court decision, *Kyllo v. United States*, perhaps reinterprets the modern Fourth Amendment "search and seizure" test established in its 1967 decision, *Katz v. United States*, which has been relied upon for the past 35 years.
4) Federal, state and local law enforcement responses to the terrorist attacks in September 2001, have blurred the lines between law enforcement, national security interests and perhaps changed the privacy rights of citizens.

SURVEILLANCE TECHNOLOGIES AND THE FOURTH AMENDMENT

In interpreting the Fourth Amendment of the Constitution, which protects, "The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures," the courts have wrestled with what constitutes a "search," and how to best protect individual privacy against intrusive or over-zealous government surveillance. In recent years, the courts have attempted to integrate law enforcement's increasing use of advanced surveillance technologies, balanced against individual privacy rights. Rules specifying when and how wiretapping can be used are one example. However, rapidly evolving surveillance technologies and their expanding use may render court decisions attempting to strike such a balance obsolete or ineffective. By the time a case winds through the judicial and appellate process, new technologies emerge, are used, and the legal premises of prior decisions must be tested all over again. Further, the surveillance technologies used in domestic law enforcement are increasingly secretive,

[§] For an overview of the legal issues surrounding the use of continuous video surveillance in public areas, see Marcus Nieto, *Public Video Surveillance: Is it an Effective Crime Prevention Tool?* (Sacramento: California Research Bureau, California State Library, June 1997), 4-6.

raising Fourth Amendment and privacy issues that can come before the courts only if their use is disclosed.

The U.S. Supreme Court decision, *Kyllo v. United States (2001)*, addresses Fourth Amendment protections and the use of advanced surveillance technologies for law enforcement purposes. While the surveillance technology at issue was not video surveillance technology, the decision still has important implications for emerging video surveillance technologies and their law enforcement applications. The following discussion briefly outlines modern Fourth Amendment law embodied in the *Katz vs. United States* decision, and then describes the *Kyllo* decision.

The Fourth Amendment of the U.S. Constitution prohibits unreasonable "searches and seizures." The 1967 Supreme Court case, *Katz vs. United States*, defined modern Fourth Amendment law.[123] In the *Katz* opinion, the U.S. Supreme Court declared: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection…[but] what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected."[124] Justice Harlan, in his concurring opinion in *Katz*, developed a two-part test recognized as the "reasonable expectation of privacy test:" first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[125] This general standard has been used to determine whether or not certain police activity and surveillance constitutes a search of an individual under the Fourth Amendment. When applied to the use of video surveillance of public streets, the prevailing view has been that video surveillance does not violate the Fourth Amendment.

One observation about *Katz* is that the reasonable test is circular. As privacy expert Jeffrey Rosen points out: "people's subjective expectations of privacy tend to reflect the amount of privacy they experience; and as surveillance technologies grew increasingly intrusive, expectations of privacy were correspondingly diminished."[126] A recent *Harvard Law Review* article noted that, "as new technologies alter individuals' privacy expectations and encroach upon realms for which society has yet to develop such expectations, the *Katz* standard becomes increasingly difficult to apply."[127] Even Justice Scalia has commented (in a dissenting opinion) that the *Katz* test is "notoriously unhelpful."[128]

In its June 2001, decision, *Kyllo vs. United States*, the U.S. Supreme Court addressed law enforcement "searches" of private homes using advanced technologies. The Court grappled with "the question of whether the use of a thermal imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment."[129] The case stemmed from federal law enforcement using a thermal imaging device to scan a home to determine whether the heat emanating from the residence was similar to heat emitted from high-intensity lamps used for indoor marijuana growth. Federal agents then obtained a warrant from a federal magistrate judge that authorized a search of Kyllo's home. The judge relied on tips from informants, utility bills and the results of the thermal imaging to issue the warrant. Kyllo unsuccessfully attempted to have the evidence (the

marijuana plants) withheld from consideration, and was indicted by a federal grand jury on one count of manufacturing marijuana.

On appeal, the Ninth Circuit sent the case back to District Court to conduct an evidentiary hearing about the intrusiveness of thermal imaging. The case then wound through a series of hearings and appellate determinations. A different Ninth Circuit panel ultimately affirmed the District Court's ruling that the thermal imaging device was not intrusive. The panel ruled that Kyllo did not have a subjective expectation of privacy because he did not keep the heat escaping his home from being detected. The panel stated "Kyllo made no attempt to conceal these [heat] emissions, demonstrating a lack of concern with the heat emitted and a lack of a subjective privacy expectation in the heat."[130] In affirming the District Court's decision, the search warrant was validated, and the marijuana plants were allowed into evidence to substantiate Kyllo's indictment. The U.S. Supreme Court chose to hear Kyllo's appeal.[131]

Justice Scalia, in writing for the five-member majority (including Justices Souter, Ginsberg, Thomas and Breyer), found that "where…the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[132]

Justice Scalia further states in *Kyllo* that

> The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable…While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes…there is ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area"…constitutes a search—at least where…the technology in question is not in general public use.[133] (citations omitted)

It is too soon to know whether, in the *Kyllo* decision, the Supreme Court "refines" *Katz* and creates a new baseline that increases privacy protection, or will continue to rely on the *Katz* test to address future privacy concerns and emerging surveillance technologies.

THE RIGHT TO PRIVACY

Personal privacy is the foundation of all freedom. Paul A. Strassmann[134]

Individual privacy in the United States is protected through a combination of constitutional guarantees, federal and state statutes, regulations, and voluntary industry codes of conduct, all of which apply to the public and private sectors in different ways.

Common Law

Governmental interest in protecting the reputation of its citizens originates in common law. The right of privacy in tort law is both protective—limiting the actions of government—and affirmative—facilitating personal expression and communication. At times, these interests may conflict: one person or industry's right to privacy may limit another's ability to gain and express information of public value. For example, private surveillance of public figures and celebrities can be controversial.

U.S. Constitution

The U.S. Constitution does not explicitly mention a right to privacy. However, as early as 1890, Justice Louis Brandeis and Samuel Warren called for a fundamental right to privacy, the "right to be left alone."[135] Justice Brandeis later wrote that privacy is "the most comprehensive of rights and the right most valued by man," a vital ingredient of human dignity.[136]

The constitutional basis for a privacy interest is "…found in the First Amendment right of association, the Fourth Amendment search and seizure guarantee, the Fifth Amendment privilege against self-incrimination, the unenumerated rights of the Ninth Amendment, and last, generally, in the penumbras which radiate from the Bill of Rights."[137] In addition, two individual interests are found in the Due Process Clause of the Fourteenth Amendment: an individual's interest in not wanting to disclose personal matters and in independently making important decisions.[138]

The First Amendment's right to freedom of speech conflicts with any right to informational privacy. Justice Brandeis and Samuel Warren acknowledged that tension, contending that privacy claims must give way where the matters published are of "general or public interest."[139] Court opinions upholding the right to informational privacy must "…dance a protean minuet around the First Amendment."[140]

The Supreme Court has recognized that Fourth Amendment protections against unreasonable search and seizure have a vital privacy component. The most well-known is in the area of an individual's interest in sexual and reproductive freedom. In *Roe v. Wade*, the U.S. Supreme Court interpreted the Bill of Rights to create "a right of personal privacy, or a guarantee that certain areas or zones of privacy exist under the Constitution."[141] Federal courts have upheld this right to privacy with respect to family planning matters, workplace privacy, and drug testing. However the courts have rejected efforts to broaden the constitutional protection beyond the "most intimate aspects of human affairs."[142] For example, the federal privacy right contains little protection for personal information and applies only to governmental actions.

In 1999, a 50-state survey of privacy statutes was conducted by the *Privacy Journal*. At that time, the federal government ranked in the "third tier" of American states.[143] The same review found that California ranks as number one for having the strongest privacy protections in the nation, based on the state's constitutional protections and "the strongest collection of laws protecting personal information."

California Constitution

The California Constitution explicitly declares that privacy is one of the inalienable rights secured to Californians, in Article I, section 1 of the Declaration of Rights:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy.**

This explicit right contrasts with the U.S. Constitution, in which the right to privacy is inferred or implicit in other rights. Ballot arguments in favor of the 1972 initiative establishing California's right to privacy stated that the provision was intended to protect two aspects of privacy: personal autonomy and prevention of disclosure of personal information.

California's right to privacy has generated the most litigation under section 1.[144] California courts have applied the privacy protection to "employment records, health records, financial records, scholastic records, and an individual's sexual history."[145]

The courts have defined three elements of a cause of action for violation of the state constitutional right to privacy action.[146] First, there must be a specific, legally protected privacy interest. Whether a privacy interest is present in a given case is a question of law. Second, there must be a reasonable expectation of privacy, a question of law and fact. Third, the gravity of the alleged invasion must be sufficiently serious, a question of law and fact. Further, privacy interests must be balanced against other important interests. For example, government actions generally must meet a higher standard than private actions.

California courts have interpreted the privacy right more generously, based on the state's Constitution, than have the federal courts.†† The California right to privacy is not limited to governmental action, as is the federal, but also applies to nongovernmental conduct (*Porten v. University of San Francisco*, 1976). It protects personal information, unlike the federal right. California courts have held that the Constitutional guarantee of privacy in Article 1, section 1 is self-enforcing and does not require implementing legislation (*White v. Davis, 1975*). Nonetheless, the California Legislature has considered and enacted numerous statutes strengthening the right to privacy.

** The right to privacy was added by ballot initiative in 1972, the only substantive amendment to the list of protected rights since its adoption in 1849.

†† A 1974 revision strengthened the independence of the state Constitution from the federal Constitution, declaring that the "rights guaranteed by this Constitution are not dependent on those guaranteed by the United States Constitution." (Section 24)

THE USA PATRIOT ACT – RECENT CHANGES IN FEDERAL LAW RELATED TO SURVEILLANCE AND TECHNOLOGY

U.S. legislative approaches to privacy traditionally have focused on protecting against the misuse of private information gathered by the government by limiting the use of personally identifiable data. For example, the government can use census data only for statistical purposes, and tax information is supposed to be highly confidential.

According to one analysis, recent federal privacy statutes have generally originated in one of two motives. The first is "…an effort by the legislative branch to address a matter left unresolved by the judicial branch…" and thereby define the scope of privacy as a legal claim.[147] Examples include the Right to Financial Privacy Act of 1978, the Privacy Protection Act of 1980 and the Electronic Communication Privacy Act of 1986. The second motive is an "…attempt to codify a legal standard for privacy for commercial transactions in new technological services." Statutory examples include the Employee Polygraph Protection Act of 1988 and the Telephone Consumer Protection Act of 1991.[148]

On October 26, 2001, Congress enacted the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (the PATRIOT Act).[149] This complex legislation has many ramifications that are beyond the scope of this report. In this section we focus briefly on those parts of the PATRIOT Act that expand:

- Law enforcement electronic surveillance
- Surveillance under the Foreign Intelligence Surveillance Act (FISA)
- Use of biometric identification systems[‡‡]

The expanded government surveillance powers authorized by the PATRIOT Act, as described in part below, have added to the debate about the appropriate balance between law enforcement, national security and civil liberties, including privacy. [150]

[‡‡] This section relies on a number of recent legal resources and commentaries across the spectrum of differing viewpoints for guidance and analysis. Resources reviewed include: United States Department of Justice, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, December 17, 2001, at http://www.cybercrime.gov/PatriotAct.htm, accessed on February 25, 2002; *U.S. Department of Justice Manual and Resource Manual* (2000); James G. Carr, *The Law of Electronic Surveillance*, 2nd ed., (1998, with 2001 Supplement): American Civil Liberties Union, "USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances," at http://www.aclu.org, accessed on February 26, 2002; Electronic Frontier Foundation, *EFF Analysis of the Provisions of the USA PATRIOT Act*, October 31, 2001, at http://www.eff.org, accessed on February 26, 2002; Tom Gede and others, *White Paper on Anti-Terrorism Legislation: Surveillance & Wiretap Laws – Developing Necessary and Constitutional Tools for Law Enforcement*, (Washington, D.C.: Federalist Society, November 2001); Brian H. Hook and others, *White Paper on Anti-terrorism Legislation Intelligence and the New Threat: The USA PATRIOT Act and Information Sharing Between the Intelligence and Law Enforcement Communities*, (Washington, D.C.: Federalist Society, December 2001); Mark Roth, "Legislation, Subpoenas, Search Warrants and Surveillance Orders—Coming to an ISP Near You?" *E-Commerce* 18, no. 7, (November 2001); The Rutherford Institute, *Forfeiting "Enduring Freedom" for "Homeland Security:" A Constitutional Analysis of the USA PATRIOT Act of 2001 and the Justice Department's Anti-Terrorism Initiatives*, (Washington, D.C.:The Institute, January 9, 2002).

Domestic Law Enforcement Surveillance Authority Expanded

Prior to recent amendments, the Electronic Communications Privacy Act of 1986 (ECPA) limited the circumstances under which federal and state government could access the contents of transactional data, both real time and stored. Congress passed Title III of the Omnibus Crime Control and Safe Streets Act in 1968 (the Wiretap Act).[151] By enacting the Wiretap Act, Congress generally prohibited private citizens from wiretapping communications of others. At the same time, the Act imposed restrictions on law enforcement using electronic surveillance to monitor communications and to gather information as evidence of criminal activity.[152] The ECPA, and the initial Wiretap Act of 1968, prohibited eavesdropping on oral, wire and electronic communications and required court orders to access subscriber and transactional data. Federal agencies were limited in their ability to access information held by the private sector, especially personal communications. Government agents were required to obtain a court order to conduct a wiretap, and postal employees could view mail content for address information only.

What types of "communications" have been defined under the Wiretap Act and subsequent amendments? Under these federal laws, communications are defined as wire,[§§] oral,[***] or electronic. Electronic communications generally excludes wire and oral.

Examples of wire communications may include communications between a mobile radio phone and a regular telephone, and cordless telephone transmissions.[153] California prohibits "malicious interception of cellular telephone transmission without the consent of all parties."[154]

Examples of electronic communications include communications of individuals in an Internet chat room (since there is no reasonable expectation of privacy in such a forum), and transmissions to digital readout pagers.[155] The *Department of Justice Manual (2000)* lists electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system."[156]

Law enforcement generally must obtain a search warrant prior to accessing electronic communications. Federal crimes investigated by using electronic surveillance generally fall into three categories: national security, very dangerous crimes and organized crime.

[§§] The "aural transfer made in whole or part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception…and such term includes any electronic storage of such communication." 18 U.S.C. 2510(1). "Aural transfer" is further defined as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. §2510 (18).

[***] "Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. §2510(2).

Wiretapping

What does electronic surveillance or wiretapping mean? The federal definition of a wiretap or "electronic, mechanical, or other device" is "any device or apparatus which can be used to intercept[†††] a wire, oral, or electronic communication.[157] The definition makes two exceptions. The first includes telephone instruments furnished by a wire/electronic communications provider to a subscriber or user who uses it in the ordinary course of business. The second is a hearing aid used to correct hearing loss to a normal level.[158]

Law enforcement first needs to obtain a wiretap order from a judge to conduct this type of surveillance. (See Appendix A for a brief description of the general process adhered to in order to obtain a wiretap order). Law enforcement may also conduct "roving" surveillance of a suspect at a number of locations by installing multiple surveillance devices. However, the process to obtain a roving wiretap order from a court includes additional steps and more information than for a fixed location wiretap order.[159]

Scope of Offenses Expanded

At the state level, federal law enables state law enforcement to obtain wiretap orders to investigate a wide array of crimes.[‡‡‡] In California, orders can be issued for investigations related to "certain drug offenses, murder, solicitation to commit murder, bombing of public property, aggravated kidnapping, and conspiracy to commit any of those offenses."[160]

Section 201 of the PATRIOT Act adds the following offenses to the scope of federal authority to obtain wiretap orders or warrants for probable cause:

- using chemical weapons
- committing violent crimes against U.S. nationals outside the U.S.
- using weapons of mass destruction
- terrorism transcending national boundaries
- financial transactions with countries designated as supporting terrorism
- providing material support to terrorists or terrorist organizations [161]

Section 202 of the Patriot Act adds felony violations and penalties for certain activities to the Computer Fraud and Abuse Act,[162] and it defines certain computer fraud and abuses as "terrorist offenses."[163] The provisions in Section 202 sunset effective December 31, 2005.

[†††] Under the statute, intercept means "the aural or other acquisition of the contents of any wire, electronic, or oral communications through the use of any electronic, mechanical or other device." 18 U.S.C. §2510(4).

[‡‡‡] State level offenses include murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other dangerous crimes dangerous to life, limb and property punishable by imprisonment for more than one year. 18 U.S.C. 2516(2).

Pen Registers and Trap and Trace Devices

Whereas the Wiretap Act regulates collecting *content* from wire and electronic communications, another federal statute regulates collecting *address* information. This statute is referred to as the Pen Registers and Trap and Trace Devices Statute.[164] Prior to the PATRIOT Act, a pen register was defined as a device that "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[165]

Section 216 of the PATRIOT Act deletes this definition and replaces it with a new one that encompasses broad communications technologies:

> A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided however, that such information shall not include the contents of any communication.

Prior to the enactment of the PATRIOT Act's Section 216, a trap and trace device was defined as, "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."[166] Under the Section 216 amendments, a trap and trace device is now defined as

> A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided however, that such information shall not include the contents of any communication.

Section 216 now allows court orders to authorize installing and using pen registers or trap and trace devices anywhere in the United States. Prior to enacting the PATRIOT Act, the scope of the order was confined to "within the jurisdiction of the court."[167]

The scope of this new expansion is broad, as Congress did not further describe "facility," "content," "routing," or "addressing." The *Department of Justice Field Guidance* indicates that "such a facility might include…a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number or similar computer network address or range of addresses."[168]

Section 216 is one of the most controversial of the PATRIOT Act, and especially raises privacy issues related to using the Internet.[169] This is in part because e-mail headers often contain content, blurring the previous distinction between address and content. Thus law enforcement may access and monitor what could be considered content information (Web surfing, URLs, Internet search engine

results). The FBI has the capability to access e-mail header and content information through its Carnivore technology (now known as DCS1000).[170]

Section 216 does provide for some accountability. When a law enforcement agency uses pen register/trap and trace devices, it must keep a record that

- identifies the officers that installed the device and had access
- indicates the date/time of installation and uninstallation
- describes the device's configuration and any modifications
- identifies any information collected by the device.

A report must be provided under seal (not available to the public) to the court that issued the order allowing the installation. Section 216 of the PATRIOT Act does not sunset, unlike several other new provisions.

User and Subscriber Information

Section 210 of the PATRIOT Act expands the types of records and information about subscribers that electronic communications service providers (ISPs) must provide to law enforcement when compelled to do so. Previously, ISPs were required to provide "basic" or non-content information such as a customer's name, address, length of service, and/or means of payment, and telephone number when presented with a subpoena by law enforcement.[171] Now, they must also provide information that may be considered as content, such as records of session times and durations, any temporarily assigned network address (Internet Protocol or IP addresses), and the means and source of payment, including any credit card or bank account number.[172]

Prior to enacting the PATRIOT Act, law enforcement needed a court order to gain access to this type of information rather than the subpoena[§§§] now required.[173] In advocating for this section, the Justice Department asserted that it "will make the process of identifying computer criminals and tracing their Internet communications faster and easier."[174]

Section 210 does not have sunset date.

Voice Mail – From Real-time Wire to Stored Electronic Communications

Section 209 of the PATRIOT Act deletes "electronic storage" from the definition of wire communications under the Wiretap Act, and inserts it into the definition of "electronic communications system" of the Electronic Communications Privacy Act.[175] These changes accomplish two important things. The status of a voice mail message system is no longer considered to be a real-time communication, like a telephone call, but rather a stored communication, such as a written document or e-mail. This definitional change

[§§§] The *Black's Law Dictionary* defines subpoena as "a command to appear at a certain time and place to give testimony upon a certain matter. A subpoena duces tecum requires production of books, papers and other things." The procedural standards that law enforcement follows in order to obtain a subpoena are not as exacting as in obtaining a warrant or a wiretap order.

means that the more stringent *wiretap order* is no longer necessary (See Appendix A for a brief description of the general process adhered to in order to obtain a wiretap order). Now only a standard search warrant is needed, with fewer limiting considerations.

The Justice Department contends that regulating stored voice communications using the wire definition, "created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable."[176] Others disagree, raising classic Constitutional questions about the balance between governmental efficiency and civil liberties, particularly Fourth Amendment protections against unreasonable searches and seizures.[177] Section 209 sunsets effective December 31, 2005.

Global Emerging Technologies – What Are They: Wire, Oral or Electronic Communications?

Civilian use and government applications of surveillance technologies, and the emerging technologies themselves, have outpaced legal debate. Here are a few questions about law enforcement, surveillance and global emerging technologies that are not adequately addressed in current statutory frameworks. An important underlying question posed by all of these examples is: What is the level of "reasonable" expectation, and protection, of privacy of the parties using these technologies?

- Some wireless cell phones may use a biometric security system (a fingerprint, for example) to enable access. What is the fingerprint: is it an address, content, or a communication? Could an ISP, or an employer, be compelled to provide that biometric identification to law enforcement conducting a criminal investigation?

- What happens to biometric information obtained by law enforcement? Will the subject under surveillance ever know that their biometric was accessed by someone else? What if the ISP or employer inadvertently provides the wrong biometric for the wrong person and both the person and the biometric end up in a criminal database? Will the federal Freedom of Information Act, or the California Public Records Act standards apply?

- How to categorize cell phones that have real-time, *audible* and video streaming capabilities via the Internet. Are they phones or computers? Is the video streaming an aural transfer? Is the communication wire or electronic?

PATRIOT Act Changes to the Foreign Intelligence Surveillance Act of 1978 (FISA)

FISA is a complex federal statute that regulates foreign intelligence investigations and surveillance in the U.S. and abroad. Historically, national security agencies and domestic law enforcement agencies using various types of surveillance have differed in their goals, their use of the information, and the manner of disclosure to the subject under surveillance. Foreign Intelligence Surveillance Court (FISC) judges hear applications for surveillance orders under FISA. The Chief Justice of the Supreme Court designates

which federal district judges become FISC judges. (Section 208 of the PATRIOT Act increases the number of such judges from seven to eleven, and mandates that at least three of them must reside within 20 miles of the District of Columbia.)[178]

FISA regulates four types of electronic surveillance:

- International communications of U.S. citizens and resident aliens
- Intercepting, within the United States, international or domestic wire communications (without the person's permission)
- Intercepting domestic-only wire or radio communications where a reasonable expectation of privacy exists and a warrant would be required
- Monitoring information other than wire or radio communications where a reasonable expectation of privacy exists and a warrant would be required [179]

Three factors contribute to determining who may authorize surveillance and how federal agencies may access the information: location of the subject (on U.S. soil or not); the FISA definition of person surveilled; and the circumstances involved.[180] Table 5 further lists these factors.

Table 5
FISA Authority Approval for Surveillance[181]

Inside United States		
FISA Definition	**Approval Authority**	**Circumstance**
United States person	FISC judge	Non-emergency
Non-U.S. person	Attorney General	Non-emergency
Either U.S. person or not	Attorney General	All emergencies
Outside United States		
U.S. person	Attorney General	Non-emergency
U.S. person	Secretary/Deputy Secretary of Defense; Secretary/Undersecretary of the Army; Director/Deputy Director of National Security Agency	Emergency
Non-U.S. person	Commanding General, Intelligence and Security Command and Designated Commanders	Non-emergency

Under FISA, a government official must certify under oath why a particular surveillance is to be conducted. Section 218 of the PATRIOT Act changes one of the related requirements from, "**the** purpose of the surveillance is to obtain foreign intelligence information" to "**a significant** purpose..."[182] This broader language may allow multiple surveillance and investigations to be included under a requested court order or warrant, and is controversial.

Section 206 inserts language into FISA that, under certain circumstances, allows surveillance to "follow" or "roam" with a person, moving from many different locations and using different types of communications technologies. (Other federal statutes already allow roaming surveillance.)[183] Section 207 extends the FISA order allowing surveillance from 90 to 120 days.[184]

Section 214 of the PATRIOT Act amends two FISA provisions related to pen registers and trap and trace devices as used for foreign intelligence and international terrorism investigations or during emergencies.[185] The controversial amendments expand: (1) the rationale under which federal officers can apply for court orders, and/or provide certifications under oath, and; (2) the types of information that can be obtained from the broader investigations.

> Each application shall…include a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person **or is relevant** to an ongoing investigation to protect against international terrorism **or** clandestine intelligence activities, provided that such investigation of a United States person is not conducted **solely** upon the basis of activities protected by the first amendment to the Constitution.[186] (emphasis added)

Previously, 50 U.S.C. §1862 provided that a court order was necessary to authorize common carriers and facilities (telephone companies and ISPs, for example) to review and release certain records in their possession for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism." Section 215 of the PATRIOT Act now provides that the F.B.I. may directly gain access to broader information by

> Mak[ing] an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment of the Constitution.[187]

Section 203 and Title IX of the PATRIOT Act generally expand information sharing between the forces in intelligence communities and domestic law enforcement. For example, Section 203 provides that:

> Any investigative or law enforcement officer, or attorney for the Government who by any means authorized…has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counter intelligence…or foreign intelligence information…to assist the official who is to receive that information in the performance of his official duties.[188]

Biometric Identification Systems

In the PATRIOT Act, Congress authorized the Attorney General to investigate the feasibility of using biometric identification systems to issue visas, and to identify "aliens who may be wanted in connection with criminal or terrorist investigations in the United States or abroad."[189]

The Justice Department Policy Guidelines for Video Surveillance

Title III (the Wiretap Act) does not cover video surveillance. However, the U.S. Department of Justice has published policy guidelines and procedures related to law enforcement video surveillance in instances when privacy is reasonably expected and protected under the Constitution. The *US DOJ Criminal Resource Manual* states that "six circuits, while recognizing that Title III does not govern video surveillance, require that search warrants for video surveillance meet certain higher, constitutional standards required under Title III."[190] The six circuits cited are the Second, Fifth, Seventh, Eighth, Ninth, and Tenth Circuits. The *US DOJ Criminal Resource Manual* states that a proposed search warrant for video surveillance under these circumstances must demonstrate probable cause (a similar requirement for a wiretap order). The Department of Justice policy also sets forth additional requirements that must be included in the warrant requested.[191]

American Bar Association Standards

Video surveillance and biometric technologies are developing at a more rapid speed than the legislative and administrative rulemaking processes that regulate law enforcement applications. To address this gap, in 1999, the Criminal Justice Section of the American Bar Association published *Standards for Technologically-Assisted Physical Surveillance* (ABA Standards).[192] The ABA Standards define ten types of surveillance devices, distinguish between covert and overt surveillance, and define terms used such as "private," "reviewing law enforcement official," and "legitimate law enforcement objective."

Of particular interest here, the "legitimate law enforcement objective" definition introduces a new regulatory concept not previously found in legislation or court decisions.[193] The language contains two elements. First, there is a general principle iterated in *Standard 2-9.1(a)*, that law enforcement surveillance should be used to "facilitate detection, investigation, prevention and deterrence of crime, the safety of citizens and officers, the apprehension and prosecution of criminals, and the protection of the innocent." Second, the surveillance should be "reasonably likely to achieve a legitimate law enforcement objective." According to Christopher Slobogin, a member of the ABA Task Force that developed the ABA Standards, the intent of including this language in the ABA Standards was to "provide the standard that police must meet in those situations not governed by the Fourth Amendment."[194] Slobogin maintains that this criterion requires "articulable reasons that the surveillance will further investigative,

deterrent, or protective ends…not a finding that a particular person will be tied to a particular crime."[****]

The ABA Standards include a section devoted specifically to video surveillance, which is defined as:

> Use of a lawfully positioned camera as a means of viewing or recording activities or conditions other than those occurring within the sight or immediate vicinity of a law enforcement official (or agent thereof) who is aware of such use.[195]

Standard 2-9.3 contains three sections that govern video surveillance of private locations, overt video surveillance of public areas, and all other "video surveillance not governed" by the prior sections.

- For video surveillance of private locations, the ABA Standards require a warrant based upon probable cause to be in issued prior to surveillance.[196]

- Overt video surveillance and other video surveillance is permissible when "a politically accountable law enforcement official" or governmental authority concludes that the surveillance will: (1) not view a private activity or condition; and (2) be reasonably likely to achieve a legitimate law enforcement objective.[197]

- When public video surveillance is used to deter rather than investigate crime, the ABA Standards suggest that the public be: (1) notified of the location and capability of the CCTV; and (2) given the opportunity to publicly comment through a hearing.[198]

Should there be Limits?

What are the appropriate limitations to CCTV video surveillance by public agencies or in public facilities? The following examples suggest the potential for abuse. In New York City, a police sergeant in Brooklyn informed on fellow officers for their improper use of CCTV cameras. According to the officer's attorney, "they were taking pictures of civilian women in the area-from breast shots to the backside."[199]

In Michigan, a newspaper reporter examining how Michigan law enforcement used the Law Enforcement Information Network (L.E.I.N.) database, found that some officers had accessed the database to stalk women, threaten motorists, and track estranged spouses. Officers had also provided information from the database to their friends who used it for similar purposes.[200]

[****] This distinction is important because it is a lower threshold than the "reasonable suspicion" standard defined in the Supreme Court decision in *Terry v. Ohio* where the Court held that an officer "must be able to point to specific and articulable facts" which warrant an intrusion. 392 U.S. 1, 21 (1968).

In Ludington, Michigan, local officials have installed real and fake video cameras in a park restroom to deter vandalism. According to the City Manager, the cameras are a necessary last resort. To ensure that individuals' rights are not violated, cameras are not aimed into stalls or urinals. Tapes are not saved or reviewed unless the bathrooms are vandalized. [201]

In 1998, New York police videotaped the Million Youth March in Harlem. In the ensuing furor over whether the tapes accurately portrayed the police response to rowdy activists, a basic issue went unaddressed. Social psychologists say that taping political events can affect a participant's self-image and desire to participate in future civic events, since being watched is associated with criminality. Ordinary citizens shy away from politics when they see activists subjected to police scrutiny.[202] Thus videotaping may discourage citizens from exercising their First Amendment right to speech, petition and assembly.

What Happens to Recorded Information?

What happens to all this recorded activity? In the case of an arrest based on recorded criminal activity, the answer is relatively clear. The video provides an officer with probable cause to arrest the recorded individual. However, there are many cases in which the recorded evidence is not straightforward and no arrest is made. There may be innocent persons on the film. Should the recording be kept? Who will have access to it? Where will the film be stored? What can it be used for? Can surveillance cameras be used to follow suspicious persons, as they engage in lawful acts and contacts, compiling a dossier of film on the way? Many of these questions were not addressed prior to the installation of public CCTV surveillance systems. As public CCTV surveillance systems continue to expand and evolve, these issues are generating public debate and are being considered by the courts and legislative bodies.

Surveillance technologies may be outpacing privacy and criminal laws, and may pose a significant threat to civil liberties. Concerned individuals range from House of Representatives Majority Leader Dick Armey to American Civil Liberties Union (ACLU) spokesman Barry Steinhardt, who contends that, "Alone, or in combination with other emerging software technology such as Computerized Face Recognition (CFR), we are creating an almost Orwellian potential for surveillance and virtually invite abuse."[203] There is a range of serious concerns, as the following quotations illustrate.

- Law professor Daniel Solove contends that, "the problem is best captured by Franz Kafka's depiction of bureaucracy in *The Trial*—a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information."[204]

- Author Gary Marx warns in his book, *Undercover: Police Surveillance in America*, "once the new surveillance systems become institutionalized and taken for granted in a democratic society, they can be used against those with the wrong political belief; against racial, ethnic, or religious minorities; and against those with lifestyles that offend the majority."[205]

RECENT STATE LAWS WITH SURVEILLANCE TECHNOLOGY IMPLICATIONS

A number of states have drafted or passed surveillance-related legislation since the 2001/2002 Fiscal Year began. A summary of the state legislation by surveillance category is as follows:

Racial Profiling Surveillance

- Michigan HB 4927 (Michigan Racial Profiling and Report Statistical Act), *Still Pending:* To fund local law enforcement agencies to purchase vehicle cameras, provide diversity training, and improve data collection.
- Minnesota SF 7, *Signed into Law*: To fund local law enforcement agencies that voluntarily participate in racial profiling study with vehicle cameras.
- South Carolina 3963, *Still Pending*: To fund law enforcement agencies that equip vehicles with cameras for traffic and pedestrian stops.
- Rhode Island HB 6100, *Signed into La*w: To purchase video surveillance cameras for ten state police cars for five years.
- Texas SB 1074, *Signed into Law:* Requires law enforcement vehicles to be equipped with surveillance cameras to record all traffic stops.

Red Light Surveillance

- Oregon HB 2380, *Signed into Law:* Allows cities with populations of 30,000 or more to use photo red light cameras.
- Alabama HB 470 (Red Light Safety Act of 2001), *Still Pending:* To fund traffic control signal and surveillance camera synchronization in certain cities to record vehicle violators.
- Arizona SB 1167, *Still Pending:* To fund traffic surveillance monitoring system and red light running program and enforcement.
- Virginia HB 1860, *Still Pending:* Authorizes the implementation of camera surveillance red light running enforcement programs.

Nursing Home Surveillance

- Texas SB 177, *Signed into law*: Requires CCTV cameras in nursing homes when it is determined that the resident needs help with communications.
- Florida SB 1202, *Signed into Law*: Permits a nursing home resident or legal representative to monitor the resident with video CCTV surveillance.
- Louisiana HB 457, *Still Pending*: Permits a nursing home resident or legal representative to install CCTV or other electronic devices in a resident's room.
- New Jersey SB 2231, *Still Pending:* Would require a nursing home to permit a resident to be monitored in the resident's room by means of an electronic device including CCTV.

School Surveillance

- Mississippi SB 2239 (Mississippi School Safety Act of 2000), *Signed into Law:* Authorizes school grants to purchase safety equipment, including CCTV cameras and other monitoring devices.

Appendix A

The primary purpose of this Appendix is to highlight procedures related to obtaining a federal wiretap order prior to Congress enacting the PATRIOT Act. Resources relied on to describe these procedures include: the *U.S. Department of Justice Manual and Resource Manual* (2000); and James G. Carr, *The Law of Electronic Surveillance*, 2nd ed. (1998; with 2001 Supplement). The information contained in this Appendix is not exhaustive.

Usually, in order to access or intercept a wire or oral communication, law enforcement must obtain a wiretap order. On a federal level, Department of Justice policy has been that federal investigative agencies submit wiretap requests first to the Department of Justice for approval by the Attorney General. The Attorney General has the authority to delegate review and approval powers of proposed orders to Deputy Assistant Attorneys General for the Criminal Division (DAAGs).[206]

Three documents must be presented to a federal judge to obtain a wiretap order: the Application, Affidavit and proposed Order. The application, or official request to the court, must be prepared by a law enforcement or investigative officer and must

- Identify the type of communications to be intercepted
- Identify the specific federal offenses
- Provide a description of the nature and location of the facilities
- Identify, specifically, the persons known to be committing the offenses and whose communications are to be intercepted
- Contain a statement that normal investigative procedures were tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ
- Contain a statement that the affidavit contains a complete statement of the facts[207]

The Affidavit must be sworn and attested to (under penalty of perjury) by an investigative or law enforcement officer. A state or local officer who is the affiant on a federal affidavit must be deputized as a federal officer of the investigating agency.[208] The Affidavit must

- Establish probable cause that the named subjects are using the location to commit the stated offenses
- Explain the need for the electronic surveillance
- Provide a detailed discussion of the investigative procedures that were tried and failed
- Contain a complete statement of any prior electronic surveillance of the same persons or location
- Contain time period for which the interception will be maintained
- Contain statement affirming that monitoring agents will minimize all non-pertinent interceptions

ENDNOTES

[1] Marcus Nieto, *Public Video Surveillance: Is it An Effective Crime Prevention Tool?* (Sacramento: California Research Bureau, California State Library, June 1997).
[2] *BusinessWeek Online*, "Privacy: What Americans Think," November 5, 2001, http://www.businessweek.com, accessed on November 9, 2001.
[3] Benny Evangelista, "Terrorist Attacks Have Inspired Nationwide Interest in Surveillance, " *San Francisco Chronicle*, September 24, 2001, E-3.
[4] John Mesenbrink, "Protecting Borders with Thermal Imaging, Infrared Plays an Important Role in CCTV," *Security Magazine*, October 20, 2001.
[5] David Banisar and Simon Davies, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice," Global Internet Liberty Campaign, 1999, at http://www.gilc.org, accessed on December 19, 2001.
[6] Doris Meissner, "The New Border Challenge Is to Reconcile Globalization with Security," *San Diego Dialogue Report* 5, no. 1 (January 2002), 3.
[7] John D. Woodward, Jr., and others. *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*, (Santa Monica: RAND, 2001), 9-10.
[8] Ibid., 11-12.
[9] John J. Weng and Daniel L. Swets, "Face Recognition," in *Biometrics: Personal Identification in Networked Society*, (Boston: Kluwer Academic Publishers, 1999), 68.
[10] P. Jonathon Phillips and others, "An Introduction to Evaluating Biometric Systems," *Computer* (February 2000), 57.
[11] Ibid.
[12] Ibid., 61.
[13] Peter Slevin, "Police Video Cameras Taped Football Fans; Super Bowl Surveillance Stirs Debate," *Washington Post*, February 1, 2001, A1.
[14] Ibid.
[15] Barnaby J. Feder, "A Surge in Demand to Use Biometrics," *The New York Times*, December 17, 2001.
[16] Press Release, "Proliferation of Surveillance Devices Threatens Privacy," Joint Statement of House Majority Leader Dick Armey and American Civil Liberties Union, July 11, 2001.
[17] "Criminal Faces in the Crowd Still Elude Hidden Cameras," *Los Angeles Times*, February 2, 2001, Home Edition, A1.
[18] Ibid., A2.
[19] John Curran, "Facial Recognition Surveillance Nothing New in Casinos," Interview with Trump Marina Casino Director, Charles Guenther, *The Associated Press State and Local Wire*, February, 25, 2001.
[20] Acres Gaming undated marketing brochure, on file with authors.
[21] Charlie Goodyear, "Some argue face recognition at Fresno's airport is too nosey," *San Francisco Chronicle*, December 17, 2001, at http://www.sfgate.com, accessed on December 17, 2001.
[22] Barnaby J. Feder, "A Surge in Demand to Use Biometrics," *The New York Times*, December 17, 2001.
[23] Ibid.
[24] Paul Foy, "Olympic Hockey Face Scan Dropped," *Los Angeles Times*, February 9, 2002, at http://www.latimes.com, accessed on February 11, 2002.
[25] Modern Security Systems of England, "British Citizens Views on the Use of CCTV Video Surveillance," 1995, in *Public Video Surveillance: Is It An Effective Crime Prevention Tool?* (Sacramento: California Research Bureau, California State Library, June 1997), 8.
[26] British Home Office Minister, John Denham, "CCTV Investment to Aid Crackdown on Crime," British Home Office Press Release, August 21, 2001.
[27] John Naughton, *The London Observer*, "Video Eyes Are Everywhere: Big Brother in Britain," Reprinted in *World Press Review* 42, no. 4, November 13, 1994, 13.
[28] Jefferey Rosen, "A Cautionary Tale For a New Age of Surveillance," *New York Times Magazine*, October 7, 2001, 3.
[29] Joel Grover, "Someone Is Watching You," *CBS2 Evening News*, New York City, November 11, 2001.
[30] William Montalbano, "Public Cameras Change Crime Picture in Britain," *Los Angeles Times*, June 6, 1996, A10.

[31] John Naughton, *The London Observer*, "Video Eyes Are Everywhere: Big Brother in Britain," Reprinted in *World Press Review*, 42; no 4, November 13, 1994, 13.
[32] M. J. Zuckerman, "Chances are, somebody's watching you," *USA Today, Tech Report*, November 30, 2000.
[33] David Skinns, "Crime reduction, diffusion and displacement: evaluating the effectiveness of CCTV," in C. Norris and others, ed., *Surveillance, Closed Circuit Television and Social Control* (Ashgate: Athenaeum Press, Ltd., 1998), 175-188. See also, Emma Short and Jason Ditton, "Seen and now heard: talking to the targets of open street CCTV," *British Journal of Criminology* 38, no. 3 (Summer 1998), 404-429.
[34] Clive Norris and Gary Armstrong, "Introduction: Watching the Watchers - Theory and Method," in *The Maximum Surveillance Society: The Rise of CCTV*, (Oxford:Berg, 1999), 95.
[35] Ibid.
[36] Jason Dutton, "Crime and the City: Public Attitudes towards Open-Street CCTV in Glasgow," *British Journal of Criminology* 40, (2000), 692-709; Nick Taylor, Closed Circuit Television: The British Experience," *Stanford Technology and Law Review* 11 (1999).
[37] Nick Tilley, "Evaluating the effectiveness of CCTV schemes," in *Surveillance, Closed Circuit Television and Social Control*, (Aldershot:Ashgate Publishing Company, 1998), 142-143.
[38] Ibid.
[39] George Radwanski, Privacy Commissioner of Canada, *News Release of Investigation of Video Surveillance Activities by the Royal Canadian Mounted Police in Kelowna, B.C.*, October 4, 2001.
[40]Fred Barbash, " The Latest From Britain: Sex, Private Lives and Videotapes," *Washington Post*, Sunday Edition, March 17, 1996, A27.
[41]Duncan Lustig-Prean, British Civil Liberties Group, Liberty, Testimony before Parliament's Media Committee, March 10, 1996.
[42]Jefferey Rosen, "A Cautionary Tale For a New Age of Surveillance, *New York Times Magazine*, October 7, 2001, 8.
[43] Marcus Nieto, *Public Video Surveillance: Is it An Effective Crime Prevention Tool? ?* (Sacramento: California Research Bureau, California State Library, June 1997).
[44] Law Enforcement Management and Administrative Statistics, 1997: *Data for Individual State and Local Agencies with 100 or More Officers*, U.S. Department of Justice, Bureau of Justice Statistics. April 1999, NCJ 171681.
[45] Jess Bravin, "Washington Police to Play 'I' Spy With Cameras, Raising Concerns," *The Wall Street Journal*, February, 13, 2002.
[46]Linda Schiffer, Maryland Governor's Office of Crime and Prevention, Press Release, "New Downtown Video Patrol Program Uses Technology To Reduce Crime," January 19, 1996.
[47] Telephone interview with Police Chief Mastorigo, Dover Township, January 2002.
[48] Telephone interview with John Brushele, Deputy Chief of Police, Tampa Bay, Florida, October 16, 1996.
[49] Barry Steinhardt and Jay Stanley, "Drawing Blanks: The Failure of Facial Recognition Technology in Tampa, Florida," *ACLU Special Report*, January 3, 2002.
[50] Statement by Lt. Greg Mullins, Virginia Beach Police Department, September 1996.
[51] Telephone interview with Trey Shull, Duty Officer, Memphis Police Department, January 2002.
[52] Press statement regarding Spenard Initative in Anchorage by Steven H. Warner, Sergeant, Anchorage Police Department, March 1995.
[53] Emelyn Cruz, "Video Cameras Shooting Down Some Crime Rates," *The Seattle Times*, July 28, 1996 B-1.
[54] M. J. Zukerman, "Chances are, Somebody's Watching You," *USA Today Tech Report*, November 30, 2000.
[55]ACLU Press Release, "Rise of Security Cameras Stirs Privacy Concerns," September 15, 1997, Reprinted from the *Washington Post* , August 28, 1997.
[56] Telephone interview with Aaron Furguson, League of California Cities, February 2002.
[57] Telephone interview with Balboa Park Ranger, Mike Ruiz, December 2001.
[58] Telephone interview with community police officer Dennis Shay, Hollywood Division of the Los Angeles Police Department, January 22, 2002.
[59] Phil Wilson, "Palm Springs Getting Surveillance Cameras; Not Everyone Smiling," *Los Angeles Times*, California Section, October 16, 2001.
[60] Telephone interview with Lt. Jo Anne West, Vallejo Police Department, February 1, 2002.

[61] Advocates For Highway and Auto Safety, *Fact Sheet: Red-Light Running Photo Enforcement*, 2001. http://www.saferoads.org.
[62] Insurance Institute For Highway Safety, *Status Report*, Vol. 36, No. 4, April 28, 2001.
[63] Barbara Boyer, Red Light Plan for Pennsylvania is Criticized, *Philadelphia Inquirer*, November 13, 2001.
[64] R. Retting, A. Williams, C. Farmer, and A. Feldman, Evaluation of Red Light Camera Enforcement in Oxnard, California, *Accident Analysis and Prevention*, 31: pages 687-694, 1999.
[65] R. Retting, A. Williams, C. Farmer, and A. Feldman, , "Evaluation of Red Light Camera Enforcement in Fairfax, Virginia", *Institute of Transportation Engineers Journal*, 69, 1999, pages 30-34.
[66] J. Fleck and B. Smith, *Can We Make Red Light Runners Stop?: Red Light Photo Enforcement in San Francisco, California*, San Francisco Department of Parking and Traffic, 1999.
[67] Advocates For Highway and Auto Safety, *Fact Sheet: Red-Light Running Photo Enforcement*, 2001. http://www.saferoads.org.
[68] Congressional Testimony by House Majority Leader Dick Armey, Before the House Transportation Subcommittee on Highways and Transit on Red Light Cameras, Washington, D.C., July 31, 2001.
[69] Comments on "The Light Running Crisis: Is It Intentional?" Office of the Majority Leader, U.S. House of Representatives, May 23, 2001.
[70] Richard Retting, "Evaluation of Red Light Camera Enforcement Signing", *Proceedings of the 2001 Annual Meeting of the Institute of Transportation Engineers*, Washington, D.C. Institute of Transportation Engineers.
[71] Dane Schiller, "You're on Transit Camera; Surveillance Debuts on VIA Buses", *San Antonio Express News*, January 23, 2001, B-1.
[72] City and County of San Francisco, Board of Supervisor Minutes, Item No. 001953, November 20, 2000.
[73]Transit Cooperative Research Program Synthesis 38, "Electronic Surveillance Technology on Transit Vehicle," Transportation Research Board, National Research Council, Washington, D.C., 2001.
[74]Ibid., 12.
[75] Joel Kugelmass and Greg McVicar, "State Computers Take A Byte Out of Privacy," *California Journal*, October 1, 1991.
[76] Mark Walbrun, Amtrak America, "Amtrak Tests Video Ticketing and Surveillance for Unmanned Stops," *High Speed Transport News* 3, no. 15, May 15, 1995.
[77] U.S. Department of Housing and Urban Development, Policy Development and Research Information Services," 1998 Picture of Subsidized Housing Facts." http://www.huduser.org/datasets.
[78] Abt Associates Inc, *Solving Crime Problems in Residential Neighborhoods: Comprehensive Changes in Design, Management, and Use*," (Washington, D.C.: National Institute of Justice, U.S. Department of Justice), April 1997.
[79]Mary Ann Wilson, State Coordinator, Virginia HUD Lines, July 2001. http://www.hud.gov/local/ric/index.html.
[80]Bill Zalud, "CCTV For Public Safety, "The Portland Story," *Security Magazine*, p. 21, October 1999.
[81] U.S. Department of Housing and Urban Development, Policy Development and Research Information Services, "A Picture of Subsidized Housing in the United States: General Description of the Data, 1998. http://www/huduser.org/datasets.
[82] Abt Associates Inc, *Solving Crime Problems in Residential Neighborhoods: Comprehensive Changes in Design, Management, and Use*," (Washington, D.C.: National Institute of Justice, U.S. Department of Justice), April 1997.
[83] Telephone interview with Tim Sciackaus, Public Housing Director, Tulare County, January 29, 2001.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87]Telephone interview, Klye Koski, Operations Director, Huntsville City Schools, Huntsville, Alabama, May 1999.
[88]Mary Green, *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies* (Washington, D.C.: National Institute of Justice, U.S. Department of Justice, September 1999.
[89] Ibid.

[90] S.A. Reid, "New watchful eyes peer into schools; Video cameras will be on when Atlanta students return to class," *The Atlanta Constitution*, August 13, 2001, 1-B.
[91] National School Safety and Security Services, "School Security Equipment and Technology, at http://www.schoolsecurity.org, accessed on December 4, 2001.
[92] Douglas Harbrecht, "We're Turning to High Tech Because It's a Quick Fix," *BusinessWeek Online*, August 31, 2000, at http://www.businessweek.com/bwdaily/dnflash/aug2000/nf20000831_230.htm, accessed on December 4, 2001.
[93] Peter Szczerba, "Advances in Protection," *American School & University*, September 1, 2000.
[94] Joe Agron and Larry Anderson, "School security by the numbers," *American School & University*, May 2000, C-6-C22.
[95] Ibid., C-9.
[96] Marcus Nieto, *Security and Crime Prevention Strategies in California Public Schools*. (Sacramento: California Research Bureau, California State Library, October 1999), 1-2.
[9730]Marcus Nieto, *Public Video Surveillance: Is It An Effective Crime Prevention Tool?* (Sacramento: California Research Bureau, California State Library, Sacramento, June 1997), 28-30.
[98] Ferman Leal, "District to focus on vandalism: Surveillance cameras to be installed at Edison High as pilot program," *Orange County Register*, March 1, 2001.
[99] Monique H. Henderson, "Moreno Valley High adds cameras," *The Press-Enterprise*, August 11, 2001.
[100] Rick Dischinger, Director of Administrative Services, quoted in Tanya Sierra, "Cameras placed to record crimes at Colton Schools," *The Press-Enterprise*, October 10, 2001.
[101] Rosemary J. Erickson, Athena Research Corporation, "Cameras and Silent Alarms: A Study of Their Effectiveness as a Robbery Deterrent," January 31, 1984.
[102]A White Paper, "From Orwell to Reality: The Role of IP-Surveillance in Modern Society," Axis Communications, June 6, 2001.
[103] Bill Zalud, "Post September 11th, Security Re-evaluates; Expects Impact Through 2002," *Security Magazine*, January 3, 2002. See also Karen Hallberg, Research Director, Cahners Publishing Company, A Division of Reed Publishing USA, "Nationwide Survey of Companies With Security Expenses," September 2001.
[104] Long Island (LI) Commercial Review, Inc., "Press Statement by Ken Darby, Executive Director, Vicon Industries, Regarding Sales of CCTV Surveillance Equipment in 1995," *LI Business News*, Section 13, Page 27, March 25, 1996.
[105]Lou Hirsh, "Spy vs. Spy: Device Takes Hidden Cameras Out of Hiding (Interview with Martin Kleckner III, President, SpyFinder LLC)," *New York City Surveillance Camera Project*, November 2001.
[106] Benny Evangelista, "Terrorist Attacks Have Inspired Nationwide Interest in Surveillance (cites official with Security Industry Association)," *San Francisco Chronicle*, Page E-3, September 24, 2001.
[107] M. J. Zuckerman, "Chances are, Somebody's Watching You," *USA Today*, November 30, 2000.
[108] Chicago Daily Law Bulletin, "Tort Law: Surveillance of Plaintiffs," *Law Bulletin Publishing Company*, April 19, 1995.
[109] Beth Givens, "A Review of Current Privacy Issues," Privacy Rights Clearinghouse, March 2001.
[110] Lewis Maltby, "Surveillance Incorporated: American Workers Forfeit Privacy for a Paycheck," An *ACLU Special Update Report*, September 1996, From Lewis L. Maltby, *A State of Emergency in the American Workplace*, National Task Force on Civil Rights in the Workplace, 1990.
[111] Aging News Alert, *The Senior Services and Funding Report*, No. 2001-18, Washington, D.C., September 24, 2001.
[112] Ibid., 6.
[113] Angelo J. Pompano, "Privacy in the Age of Video Surveillance; This is Not Your Father's Candid Camera," Yale-New Haven Teachers Institute, 2001, 4.
[114] Sandra Stokley, "Hidden Camera Lawsuit Sent to High Court," *The Press Enterprise* (Riverside, CA), September 14, 2001.
[115] *California Acrylic Industries, Inc. v. National Labor Relations Board*, 150 F.3d 1095 (9th Cir. 1998).
[116] White Paper, *From Orwell to Reality: The Role of IP-Surveillance in Modern Society*, AXIS Communications, June 6, 2001.
[117] Rosemary J. Erickson, Ph.D., "Convenience Store Security at the Millennium, *National Association of Convenience Stores*, February, 1998.
[118] Ibid., 44.

[119] California Department of Industrial Relations, Division of Occupational Safety and Health, *Model Injury and Illness Prevention Program for Workplace Security*, 1995.
[120] Benny Evangelista, "Terrorist Attacks Have Inspired Nationwide Interest in Surveillance, " *San Francisco Chronicle*, September 24, 2001, E-3.
[121] Robert D. Bickel, *Briefing Paper on the Legal Issues Related to Silent Video Surveillance*, (Washington, D.C.: Security Industry Association and Private Sector Liaison Committee, April 8, 1999) at http://www.npr.org, accessed on February 24, 2002, 39-45.
[122] *Kyllo v. United States*, 121 S.Ct. 2038 (2001).
[123] 389 U.S. 347 (1967).
[124] Ibid., 359.
[125] Ibid.
[126] Jeffrey Rosen, "A Victory for Privacy," *Wall Street Journal*, January 18, 2001, A18.
[127] *Harvard Law Review Note*, 115 no. 1 (November 2001), 346.
[128] *Minnesota v. Carter*, 525 U.S. 83, 97 (1998).
[129] 121 S. Ct. 2038, 2040 (2001).
[130] *United States v. Kyllo* 190 F.3d 1041, 1046 (9th Cir., 1999).
[131] Ibid., 2041.
[132] 121 S. Ct. 2038 (2001).
[133] Ibid.
[134] Paul A. Strassmann, *The Politics of Information Management*, (New Canaan: The Information Economics Press, 1995), 197.
[135] Warren and Brandeis, "The Right to Privacy", 4 *Harvard. L. Rev*. 193 (1890).
[136] *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[137] Jerome A. Barron and C. Thomas Dienes, *Handbook of Free Speech and Free Press*, (Boston: Little, Brown and Company, 1979), 370.
[138] Nancy A. Novak, "Jury on Trial: Juror's Constitutional Right to Privacy Falls Under Scrutiny of the Courts," *San Diego Justice Journal*, Winter 1995.
[139] Warren and Brandeis, 214.
[140] Gary Williams, "Symposium: The Right of Privacy Versus the Right to Know: The War Continues," *Loyola of Los Angeles Entertainment Law Journal*, 1999.
[141] *Roe v. Wade*, 410 U.S. 113, 152, 93 S.Ct. 705,726 (1973)
[142] *McNally v. Pulitzer Publishing Co*., 532 F.2d 69 (8th Cir.), *cert. denied*, 429 U.S. 855 (1976).
[143] Privacy Journal, *Ranking of States in Privacy Protections*, October 7, 1999, http://www.townonline.com/privacyjournal.
[144] Joseph R. Grodin, Calvin R. Massey, and Richard B. Cunningham, *The California State Constitution; A Reference Guide*, Greenwood Press, 1993.
[145] Barron and Dienes, 24.
[146] See *Hill v. National Collegiate Athletic Assn*. (1994) 7 C.4th 1, C.R. 2d 834, 865 P.2d 633, in Bernard E. Witkin, *Witkin Summary of California Law*, Ninth Edition, Chapter XI, II, 1998.
[147] Marc Rotenberg, *Privacy Law Sourcebook 1999*, Electronic Privacy Information Center, Washington, D.C., i, ii.
[148] Ibid.
[149] Public Law 107-56 [H.R. 3162].
[150] The Rutherford Institute, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act of 2001 and the Justice Department's Anti-Terrorism Initiatives*, (Charlottesville:The Institute, January 9, 2002), 13.
[151] 18 U.S.C. §§ 2510-22.
[152] U.S. Department of Justice, *The Department of Justice Manual*, (Gaithersberg: Aspen Law & Business, 2000) Title 9-Electronic Surveillance, Title 9-123-124.
[153] James G. Carr, *The Law of Electronic Surveillance*, 2nd ed., (Deerfield: Clark Boardman Callaghan, 1998), 3-5 – 3-7, citations omitted.
[154] Ibid., 3-15, citing Cal. Penal Code§632.5.
[155] Ibid., 3-25 – 3-26.
[156] U.S. Department of Justice, *The Department of Justice Criminal Resource Manual* No. 1045, (Gaithersberg: Aspen Law & Business, 2000), Title 9-1644 (*US DOJ Criminal Resource Manual*).

[157] 18 U.S.C. §2510(5).
[158] *US DOJ Criminal Resource Manual* No. 1047, Title 9-1646.
[159] James G. Carr, *The Law of Electronic Surveillance*, 2nd ed., 4-50 – 4-53.
[160] Carr, citing Cal. Penal Code 629.52(a).
[161] 18 U.S.C. §2516.
[162] 18 U.S.C. §1030.
[163] 18 U.S.C. §2516(1); 18 U.S.C. §1030.
[164] 18 U.S.C. §§ 3121-27.
[165] 18 U.S.C. §3127(3).
[166] 18 U.S.C. §3127(4).
[167] 18 U.S.C. §3123(a)(1).
[168] United States Department of Justice, *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, December 17, 2001, at http://www.cybercrime.gov/PatriotAct.htm, accessed on February 25, 2002 (*DOJ Field Guidance*), 3-4.
[169] Tom Gede and others, *White Paper on Anti-Terrorism Legislation: Surveillance & Wiretap Laws-Developing Necessary and Constitutional Tools for Law Enforcement*, (Washington, D.C.: The Federalist Society, November 2001), 7-8.
[170] "Personal Privacy vs. National Defense: The State of Government Surveillance Since September 11," in *Smart Computer Privacy & Security* 8, no. 4 (2002), 53-54.
[171] "Is Your ISP On Your Side? When It Will and Will Not Protect Your Privacy" in *Smart Computing: Computer Privacy & Security* 8, no. 4, (2002), 104.
[172] 18 U.S.C. § 2703(c).
[173] "Is Your ISP On Your Side? When It Will and Will Not Protect Your Privacy" in *Smart Computing: Computer Privacy & Security* 8, no. 4, (2002), 103-105.
[174] *DOJ Field Guidance*, 2.
[175] 18 U.S.C. §2510(1); 18 U.S.C. §2703(1).
[176] *DOJ Field Guidance*, 1.
[177] Tom Gede and others, *White Paper on Anti-Terrorism Legislation: Surveillance & Wiretap Laws – Developing Necessary and Constitutional Tools for Law Enforcement*, (Washington, D.C.: Federalist Society, November 2001), 10.
[178] 50 U.S.C. §1803.
[179] James G. Carr, *The Law of Electronic Surveillance*, 2nd ed., 9-6.1 – 9.8; 50 U.S.C.§1801(f).
[180] Major Louis A. Chiarella and Major Michael A. Newton, '"So Judge, How Do I Get that FISA Warrant?': The Policy and Procedure for Conducting Electronic Surveillance," *The Army Lawyer* Pamphlet 27-50-299 (October 1997), pp. 32-33.
[181] Ibid.
[182] 50 U.S.C. § §1804(7)(A)(B); 1823((a)(7)(B).
[183] 18 U.S.C. §2518(11)(b)(ii).
[184] 50 U.S.C. §1805(c).
[185] 18 U.S.C. §§ 1842(c)(2); 1843(b)(1).
[186] Ibid.
[187] 50 U.S.C. §501(a)(1) (formerly 50 U.S.C. §1862).
[188] 18 U.S.C. §2517(6).
[189] USA PATRIOT Act, P.L. 107-56, §1008.
[190] *U.S. Department of Justice Criminal Resource Manual* No. 32, Title 9-618.
[191] Ibid.
[192] Criminal Justice Section, American Bar Association, "Electronic Surveillance: Part B: Technologically-Assisted Physical Surveillance Standard 2-9.3 Video Surveillance", 1999, at http://www.abanet.org/crimjust/standards/taps_blk.html, accessed on January 14, 2002.
[193] Christopher Slobogin, "Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards," *Harvard Journal of Law and Technology* 10, no. 3 (Summer 1997), 416-418.
[194] Ibid., 416.
[195] ABA Standard 2-9.2 (j), p. 15.
[196] ABA Standard 2-9.3(a), pp. 15-16.

[197] ABA Standard 2-9.3(b)-(c), p. 16.
[198] Ibid.
[199] Barry Steinhardt, "ACLU Calls on Law Enforcement to Support Privacy Laws for Public Video Surveillance," American Civil Liberties Union, Press Release, April 8, 1999.
[200] M.L. Elrick, "Cops tap database to harass, intimidate," *Detroit Free Press*, July 31, 2001. At http://freep.com/news/mich/lein31_20010731.htm.
[201] Angelo J. Pompano, "Privacy in the Age of Video Surveillance; This is Not Your Father's Candid Camera," Yale-New Haven Teachers Institute, (2001), 4.
[202] Mark Boal, "The Surveillance Society: Spycam City," *The Village Voice*, October 6, 1998.
[203]Barry Steinhardt, "ACLU Calls on Law Enforcement to Support Privacy Laws for Public Video Surveillance," American Civil Liberties Union, Press Release, April 8, 1999.
[204] Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors from Information Privacy," *Stanford Law Review* 53, no.6(July 2001) 1398.
[205] Gary Marx, *Undercover: Police Surveillance in America*, University of California Press, Berkeley, CA, Page 96, 1998.
[206] *US DOJ Manual* 9-7.100, Title 9-124.
[207] 18 U.S.C. §2518; US DOJ Criminal Resource Manual No. 28. Title 9-610,11.
[208] 18 U.S.C. §2516(1).